#4

⑲ 日本国特許庁

公開特許公報

⑪特開昭 51-108701

㊸公開日 昭51.(1976) 9.27

㉑特願昭 51-16096

㉒出願日 昭51.(1976) 2.18

審査請求 有 (全32頁)

庁内整理番号

6964 53
7240 53
7165 56

㊷日本分類

96(1)D0
96(7)A1
97(7)E2

㊶Int.Cl²

H04K 1/00
H04L 9/00
G06F 3/00

Best Available Copy

優先権主張
国名 アメリカ合衆国
出願 1975年2月24日
出願番号 第553264号

特許願(1)

昭和51年2月18日

特許庁長官 片山石郎殿

1.発明の名称

アンプリファイ
暗号装置

2.発明者

住所 アメリカ合衆国ニューヨーク州ハーレー、
オーバールック・ドライブ5番地
氏名 ワイリアム・エフ・エイルアム(他4名)

3.特許出願人

住所 アメリカ合衆国10504、ニューヨーク州
アーモンク(番地なし)
名称 インターナショナル・ビジネス・マシーンズ コーポレーション
(709)
代表者 ジェイ・エイナ・グレイディー
国籍 アメリカ合衆国

4.代理人

住所 郵便番号 106
東京都港区六本木三丁目2番12号
日本アイ・ビー・エム株式会社
Tel(代表)586-1111
氏名 弁理士 小野 俊一
(6454)

5.添付書類の目録

(1)	明細書	1通
(2)	図面	1通
(3)	委任状及訳文	各1通
(4)	優先権証明書及訳文	各1通
(5)	出願審査請求書	1通

51.2.19

明細書

1.発明の名称 暗号装置。

2.特許請求の範囲

(1) 一組の暗号キー・ビットの制御のもとにデータ・ビットのブロックに対して該ブロック暗号処理操作を実行するための暗号装置にして、

上記データ・ビットのブロックを記憶するための記憶手段と、

上記一組の暗号キー・ビットを置換して出力するための第1線形変換手段と、

上記記憶手段に接続され、上記データ・ビットのブロックを拡張することによつて、上記第1線形変換手段から出力された暗号キー・ビットの数に等しいデータ・ビットのブロックを生成するための手段と、

該手段からの拡張されたデータ ビットのブロック及び上記第1線形変換手段からの置換された暗号キー・ビットに従つて代替変換を実行することにより、元のデータ・ビットの数に等しいビット数を有する代替ビット群を生成するための手段と、

該手段から出力された上記代替ビット群を置換することにより、上記データ ビットのブロックの該ブロック暗号を生成するための第2線形変換手段とを有することを特徴とする暗号装置。

(2) 上記代替ビット群を生成するための手段が、

拡張されたデータ ビット及び置換された暗号キー ビットを組合わせて新しい一組のビットを生成するための手段と、

該手段から出力された上記一組のビットに対して非線形代替変換を施すことにより上記代替ビット群を生成するための非線形変換手段とより成ることを特徴とする特許請求の範囲第1項記載の暗号装置。

3.発明の詳細な説明

本発明は、データ処理環境のもとで利用される暗号装置に関するものであり、更に具体的には、データの機密保護及びプライバシーを確立するために、ディジタル・データを暗号化したり解読したりするのに使用され得る積ブロック暗号プロセスを遂行するための暗号装置に関するものである。

コンピュータ・システム・ネットワークにおける遠隔通信の利用、端末即ち入出力装置と制御装置との間の非常に長いケーブル接続の使用、及び記憶媒体の移動可能性が各々増大するにつれて、データの物理的な保護が一般に保証され得なくなつてきたために、データの盗受又は変更における関心が高まつてきた。暗号方式は、データの伝送媒体よりもむしろデータ自身を保護するという点において、データの機密性及びプライバシーの保護を達成するための1つの手段として認められている。

これまでにも、データ通信の機密保護及びプライバシーの維持を目的として、メッセージを暗号化するための種々のシステムが開発されている。このようなシステムの1つに、ブロック全体が所定の暗号キーに従つて代替（substitute）されるようなブロック暗号システムがある。代替されたメッセージは、暗号キーを知らなければ理解され得ない暗号テキストになる。所定の暗号キーに従つて処理が行なわれる代替技術（substitution technique）の利点は、この暗号キーを逆に応用することによつて解読操作を簡単に実行できることにある。代替技術の設計及び原理に関する更に詳しい説明は、例えば1949年10月に発行されたBell System Technical Journal，第28巻、第656～715頁に掲載されているC. E. Shannonによる"Communication Theory of Secrecy Systems"と題する論文及び1973年5月に発行されたScientific American，第228巻、第5号、第15～23頁に記載されているH. Feistelによる"Cryptography and Computer Privacy"と題する論文に見出される。これら2つの論文には、2以上の暗号が、例えば非線形代替及びこれに続く線形変換といつた連続的な段階によつて、連続的に組合わされるような積暗号システムについての詳しい説明がなされている。

データ処理システム内でのデータの機密保護及びプライバシーを改善するため、種々の積暗号システムが開発されてきた。例えば米国特許第3798359号明細書には、非暗号テキスト・メッセージ（暗号化されていないメッセージ）の線形変換及び非線形変換を組合わせる積暗号システムが開示されている。これらの変換は、一意的な暗号キーを用いて行なわれ、このキーの関数になつている。暗号キーは、変換を制御することの他に、暗号システム内で種々のレジスタ代替及び部分的に暗号化されたデータのモジュロ2加算の制御も行なう。しかしながら、上記米国特許明細書には、キー経路指定器によるモジュロ2加算器への暗号キー・ビットの正確なマッピングの詳細や、代替機能ボックス内で実行される特別の非線形変換又は分散器（diffuser）によつて実行される特別の置換（permutation）の詳細しこれらはすべて暗号処理操作の質に重大な影響を及ぼすものである）については、何ら開示されていない。暗号キーは、幾つかの小さなグループに分けられ、各グループに含まれる暗号キー・ビットは、暗号処理操作が繰返される度にシフトされる。各グループに含まれる暗号キー・ビットの数が比較的少ないため、各暗号キー・ビット・グループの反復する効果は、暗号処理操作の施られた部分に限定される。これもまた、暗号処理操作の質に影響を及ぼすものである。更にこのシステムでは、暗号キー・ビットのみの関数として選択された2種類の代替機能ボックスだけが使用されているが、これも同様に暗号処理操作の質に影響を及ぼすものである。

上記のシステムに関連して、米国特許第3796830号明細書には、非暗号テキストのブロックがセグメント単位で処理されるような積暗号システムが開示されている。各セグメントは、暗号キーの一部に従つて、選択に変換される。しかし

ながら、このシステムはその性質において直列式であるためにスループット速度が遅く、またもしこれを並列式に変更しようとすれば、そのハードウエアはかなり複雑になる。更に、前述のシステムと同様に、このシステムもまた同じような2種類の代替機能ボックスのみに限定される。

本発明に従えば、任意に選ばれた1つの暗号キーの制御のもとに、32ビットのデータ・ブロックを暗号処理（暗号化又は解読）し得る暗号装置が提供される。この暗号装置は、全部で52個のデータ・ビットを有し且つ各々が4個のデータ・ビットより成る8個のセグメントに分けられたデータ・ブロックが、6個のデータ・ビットを各々有する8個のセグメントを構成する48個のデータ・ビットのブロックへ拡張されるような操作を実行することにより、暗号処理を行なう。このようなデータ・ビットの拡張は、8個の4ビット・セグメントの各々のエンド・データ・ビット、例えば最初の2ビットを二重にすることによつて達成される。8個の6ビット・セグメントとみなされる拡張された48個のデータ・ビットは、任意に決められた置換に従つて選択された、8個の6暗号キー・ビット・セグメントとみなされる48個の暗号キー・ビットとモジュロ2加算によつて組合わされる。モジュロ2加算の結果の8個の6ビット・セグメントは、8種類の非アフィン変換のための変換の引数を構成する。各変換操作においては、先行の6ビット・セグメントの二重にされたエンド・ビット及び置換された暗号キー・ビットのモジュロ2加算と、後続の6ビット・セグメントの二重にされたエンド・ビット及び別の置換された暗号キー・ビットのモジュロ2加算との結果として生じた6ビット・セグメントの2個のエンド・ビット（両端のビット）が解読されて、各々16個のエントリーを有する4個の機能テーブルのうちの1つが選択される。各エントリーは4ビットから成つている。次に、この6ビット・セグメントの残り4個のビットを解読することにより、選択された機能テーブルの16個の4ビット・エントリーのうちの1つが選択される。各セグメントに対する置換操作に貢与する機能テーブルは互いに異なつており、従つて、8種類の異つた置換操作が行なわれて、32ビットの代替セットを規定する8個の4ビット・セグメントが生じる。なお、本明細書において、「代替」とは或るビット・ブロックが別のビット・ブロックへ代えられることを意味し、「置換」とは或るビット・ブロック内においてビットの順序が変更されることを意味する。次に、この32ビットの代替ビットは、任意に決められた置換による線形変換を受ける。このような非線形置換及び線形置換の組合わせにより、32ビットのデータ・ブロックの新ブロック暗号が生成される。

上述の新ブロック暗号処理操作は、暗号関数及びキー・スケジュール関数によつて規定され得る新ブロック暗号処理アルゴリズムに従つて、16回繰返して実行される暗号化プロセスに使用され得る。かくして、暗号化プロセスにおいて、もし64ビットの入力メッセージ・ブロックが32ビットの1ブロックL及び32ビットの1ブロックRから成つていると、この入力メッセージ・ブロックは項LRで表わされる。また、もし暗号キー・ビットのブロックが暗号キーKEYから選ばれるならば、このブロックは項Kで表わされる。従つて、最後のものを除くすべての繰返しについては、入力がLRの時の出力は項L'K'で表わされる。これは、次のように定義され得る。

$$L' = R$$
$$K' = L \oplus t(R, K) \qquad (1)$$

上式において、⊕はビット毎のモジュロ2加算（排他的オア）を表わし、各繰返し操作の間に、暗号キーKEYから暗号キー・ビットの異なつたブロックKが選ばれる。最後の繰返しを除く各繰返

し段に出力が互換（transpose）されるので、入力がLRの最後の繰返しにおける出力は、次式で定義され得る項L'R'で表わされる。

$$L' = L \oplus f(R, K)$$
$$R' = R \quad (2)$$

更に、もしキー・スケジュールKSが1から16までの範囲にある整数n及び暗号キーKEYの関数として定義されるならば、暗号キーKEYからの暗号キー・ビットの置換された選択は、次式で定義される項Knによって表わすことができる。

$$K_n = KS(n, KEY) \quad (3)$$

かくして、L_{n-1}及びR_{n-1}が各々L及びRの時に、もしL_0及びR_0が各々L及びRであり且つL_n及びR_nが各々L'及びR'であれば、nが1から15までの範囲にある場合の繰返し操作の出力は次式で定義され得る。

$$L_n = R_{n-1}$$
$$R_n = L_{n-1} \oplus f(R_{n-1}, K_n) \quad (4)$$

最後の繰返し操作の出力は互換されないので、nが16の時の最後の繰返し操作の出力は次式で定義され得る。

$$L_n = L_{n-1} \oplus f(R_{n-1}, K_n)$$
$$R_n = R_{n-1} \quad (5)$$

暗号化プロセスにおいては、K_1が最初の繰返しで使用され、K_2が2回目の繰返しで使用され、以下同様にして、最後の16回目の繰返しではK_{16}が使用される。本発明に従う積ブロック暗号処理アルゴリズムを利用するこのような暗号化プロセスの一例が第8図に示されている。

暗号関数f(R、K)は、選択関数と呼ばれる原始関数及び置換関数によって定義され得る。かくして、もし32ビットのブロックRが48ビットのブロックへ拡張されるならば、拡張されたブロックは項E(R)で表わされる。この拡張されたブロックE(R)は、任意に決められた置換に従って選択された暗号キー・ビットのブロックKとモジュロ2加算で組合わされ、8個の6ビット・セグメントB1、B2、…B8が生成される。これらのセグメントは、8種類の異なった選択関数S1、S2、…S8に対する引数を構成する。従って、モジュロ2加算は次のように定義され得る。

$$E(R) \oplus K = B1, B2, B3, B4, B5, B6, B7 \text{及び} B8 \quad (6)$$

各選択関数S_iは、6ビット・セグメントBiを4ビット・セグメントへ変換し、このため8個の異なった選択関数はS1(B1)、S2(B2)、S3(B3)、S4(B4)、S5(B5)、S6(B6)、S7(B7)及びS8(B8)として定義され得る。次に、8個の選択関数の8個の4ビット・セグメント出力は、32ビットの単一ブロックへ統合される。この32ビット・ブロックは、置換関数Pによって、次のように表わされる新しい32ビットのブロックへ変換される。

$$P(S1(B1), S2(B2), \cdots, S8(B8)) \quad (7)$$

これが暗号関数f(R、K)を表わす。

本発明に従う積ブロック暗号処理操作は、前と同じように暗号関数及びキー・スケジュール関数によって規定され得る積ブロック暗号処理アルゴリズムに従って、16回繰返して実行される解読プロセスにも使用され得る。かくして、もし暗号化された64ビットの入力メッセージ・ブロックが、32ビットの1ブロックL'及び32ビットの1ブロックR'から成っていると、この暗号化された入力メッセージ・ブロックは項L'R'で表わされる。従って、入力がL'R'の最初の繰返しにおける出力は、互換された後で項LRで表わされ得る。これは、次のように定義することができる。

$$L = L' \oplus f(R, K)$$
$$R = R' \quad (8)$$

この場合、各繰返し後に暗号キーKEYから選ばれる暗号キー・ビットの異なったブロックKは暗号化操作の時に選ばれた順序とは反対の順序で

通される。最初の繰返し後は、後続の各繰返しは最後のものを除いて互換され、従つて入力がL' R' の後続の各繰返しにおける出力は、次の式で定義される函しRによつて表わすことができる。

$$L = R' \oplus f(L', K) \qquad (9)$$
$$R \sim L'$$

かくして、もしLn及びRnが各々L及びRであり且つLn-1及びRn-1が各々L' 及びR' であれば、nが16に等しい時の最初の繰返しの出力は次のように表わすことができる。

$$L_{n-1} = L_n \oplus f(R_n, K_n) \qquad (10)$$
$$R_{n-1} = R_n$$

最後の繰返しを除く各繰返し後に出力が互換されるので、nが15から1までの範囲にある場合の後続の各繰返しの出力は次式で定義され得る。

$$L_{n-1} = R_n \oplus f(L_n, K_n) \qquad (11)$$
$$R_{n-1} = L_n$$

解読操作においては、最初の繰返しにK16 が使用され、2回目の繰返しにK15が使用され、以下同様にして、16回目の繰返しではK1 が使用される。本発明に従う積ブロック暗号処理アルゴリズムを利用するこのような解読プロセスの例が第6図に示されている。

従つて本発明の目的は、暗号キーの制御のもとにデータ ブロックを暗号処理するための暗号装置を提供するにある。

本発明の他の目的は、暗号キーの制御のもとにディジタル・データを暗号処理するための積ブロック暗号処理プロセスを提供するにある。

本発明の他の目的は、暗号キー及びディジタル・データに従つて制御される非線形変換を含む積ブロック暗号処理プロセスを提供するにある。

本発明の他の目的は、多数対1の非線形変換を含む積ブロック暗号処理プロセスを提供するにある。

本発明の他の目的は、暗号処理されるべきデータ・ビットのブロックが、これらのデータ・ビットのうちの所定のものを二重にすることによつて拡張されるような、また一組の暗号キー・ビット並びに一組のデータ ビット及び二重にされたデータ・ビットに従つて制御される非線形変換機能を含むような積ブロック暗号処理プロセスを提供するにある。

本発明の他の目的は、暗号処理されるべきデータ・ビットの一群の並列セグメントが、各セグメント中のデータ・ビットの所定のものを二重にすることによつて拡張されるような、また一組の暗号キー・ビットを含む一群の並列セグメント並びにデータ・ビット及び二重にされたデータ ビットを含む一群の並列セグメントに従つて制御される一群の非線形変換機能を含むような積ブロック暗号処理プロセスを提供するにある。

前にも触れたように、データ処理ネットワークの内部においては、データの傍受又は変更や、記憶媒体の物理的取外しに対して、ネットワークを物理的に保護することは極めて困難である。この問題は、データが通信線を介して処理装置と遠隔制御ユニット又は遠隔端末との間でやりとりされる場合、非常に長いケーブル接続を介して制御ユニットと端末即ち入出力装置との間でやりとりされる場合、又は移動可能な記憶媒体が設置されている場合において最も顕著に生じる。このような状況のもとでデータの機密保護を達成し、プライバシーを守るための1つの手段として、ネットワーク内の重要な場所に暗号装置が設置される。送信局においては、暗号化モードで動作する暗号装置によつて非暗号データが暗号化された後、この被暗号化データが受信局の方へ伝送される。受信局側では、解読モードで動作する暗号装置を用いて、伝送されてきた被暗号化データを解読することにより、元の非暗号データが得られる。受信局及び送信局の役割が反対になつた時、即ち今まで

受信局として働いていたところが送信局になり且つ送信局として働いていたところが受信局になつた時には、各々の局に設置されている暗号装置も同様に今までとは反対のモードで動作される。第1図は、代表的なデータ処理ネットワークにおける暗号装置の設置場所を例示したものである。第1図の例では、暗号装置は黒い丸印の部分に設置されている。

第2図は、8バイトから成る64ビットのデータ・ワードDW即ちデータ・メッセージ・ブロックを暗号化又は解読するための暗号装置を示したものである。図において、太い実線の途中にある丸印で囲まれた数字は、各々の母線を介して送られるビットの数を表わしている。各バイトは8個のデータ・ビットを含んでいる。メッセージ・ブロックのデータ・バイトは、データ・バス・インを介して一時に1つずつ逐次に暗号装置へ印加され、従つて、64ビットのメッセージ・ブロックを完全に転送するには、8サイクルを必要とする。暗号装置に受信された各バイトは、通常の交差配線ボックス50（以下、Pボックスという）によつて実行される初期順形置換（ビット順序の変更）を受ける。次いで、各々の置換されたデータ・バイトは2つに分割されて、偶数番目のビット0、2、4及び6が上部入力バッファ（以下、UIBと略す）100に印加され、奇数番目のビット1、3、5及び7が下部入力バッファ（以下、LIBと略す）150に印加される。UIB100及びLIB150は、直列－並列変換を実行し、従つて、メッセージ・ブロックの8バイトが受信された後に、UIB100はメッセージ・ブロックの第1半分の32ビットを上部データ・レジスタ（UDR）200へ並列に供給し、一方LIB150はメッセージ・ブロックの残り32ビットを下部データ・レジスタ（LDR）250へ供給する。

64ビットのメッセージ・ブロックが受信されて、UIB100及びLIB150へバッファされている時に、各々が7個のキー・ビット及び1個のパリティ・ビットを含む8個のキー・バイトを供給する64ビットの外部レジスタから暗号キーが入力される。この暗号キーの各暗号キー・バイトは、8番目のビット即ちパリティ・ビットを除いて、一時に7ビット・バイトずつキー・バス・インを介して暗号装置へ印加される。この場合も、暗号キーを完全に転送するには、8サイクルを必要とする。上述のメッセージ・ブロックと同様に、暗号装置に受取られた各暗号キー・バイトもPボックス500による初期置換を受け、この後、暗号キーの各々の置換されたバイトは2つに分割されて、各7ビット・バイトの最初の4ビットが上部キー・レジスタ（UKR）350へ印加され、残りの3ビットが下部キー・レジスタ（LKR）400へ印加される。UKR350及びLKR400は各々28個の段を含み、UKR350の最後の段がLKR400の25番目の段に接続されている。UKR350及びLKR400は共に直列－並列変換を行ない、8個の7ビット・バイト（各々が8ビットを含む7個のグループと考えられる）が逐次に受取られている間に、これら7グループのうちUKR350の段1、8及び16へ各々連次に受取られた8ビットより成る3グループと、LKR400の段0、8及び16へ各々連次に受取られた8ビットより成る3グループとが、各々3個の並列8ビット・グループへ変換される。これら2つの3グループは、UKR350及びLKR400における24ビットの2つの並列グループとみなされ得る。7個の8ビット・グループの残りのグループは、UKR350の段24へ逐次に受取られる。UKR350の後続の段LKR400の段24とが接続されているので、UKR350へ逐次に受取られた残りの8ビット・グループの最初の4ビットは、LKR400へ送られて、その後続の4段において4ビットの並列4分グループへ変換され、次の4ビットはUKR350の後続の4段において4ビットの並列4分グループへ変換される。かくして、UKR350及びLKR400は、各々が28ビットの2個の並列グループとみなされる暗号キーを含む。

この時点においては、メッセージ・ブロックの第1半分及び第2半分が各々UDR200及びL

DR250へ転送され。そしてUKR350及びLKR400には暗号キーがロードされているが。一はUKR350及びLKR400へロードされると。これら2つのレジスタ間の転送はこれ以上使用されず。UKR350及びLKR400は。各々28ビットの独立したシフト・レジスタとして動作する。暗号化プロセスにおいては。UKR350及びLKR400の暗号キー内容が1ビット位置走行単向シフトされた後に。16回のふみし操作が連続的に実行される。暗号化プロセスの繰返し操作(最初のものを除く)の間に。UKR350及びLKR400の暗号キー内容は1又は2ビット位置だけシフトされる。各レジスタは所定のシフト計画に従つて。暗号化プロセスの間に常に28ビット位置シフトされるので。この手順は暗号キー・ビットの順位を置列を確実に行なわせるものである。

暗号化動作の最初の繰返しにおいては。UDR200に含まれるメッセージ・ブロックの第1半分(32個のデータ・ビットを含み。これらは各々4個のデータ・ビットより成る8個のセグメントとみなされる)は。各々6個のデータ・ビットをそれ8個のセグメントを形成する48個のデータ・ビットへ拡張される。この拡張は。8個の4ビット・セグメントの各々のエンド・ビットを二重にすることによつて達成される。拡張された48個のデータ・ビット(8個の6ビット・セグメントを構成するものと考えられる)は。8個のモジュロ2加算器500～514へ並列に印加される。各モジュロ2加算器は6個の独自的オア回路より成つている。これと同時に。56個の暗号キー・ビットのうち。UKR350から選択された24個のキー・ビット及びLKR400から選択された24個のキービットより成る48個の所定の暗号キー・ビットは。Pボックス450において独自置換(一定)された後。8個の6暗号キー・ビット・セグメントとして。8個のモジュロ2加算器500～614の独自的オア回路へ並列に印加される。8個のモジュロ2加算器500～514は。8個の6ビット・セグメントを構成するものと考えられる拡張された48個のデータ・ビットと。同じく8個の6ビット・セグメントを構成するものと考えられる置換された48個の暗号キー・ビットとを並列的に組合わせて。8個の部アフィン強度機能ボックス(以下。Sボックスという)550～564のための選択の引数を構成する8個の6ビット・セグメントを出力する。各Sボックスは評価形変換を実行する。各Sボックスにおいては。先行の6ビット・データ・セグメントの二重にされた1エンド・ビット及び選択された1暗号キー・ビットのモジュロ2加算と。該後の6ビット・データ・セグメントの二重にされた1エンド・ビット及び別の選択された1暗号キー・ビットのモジュロ2加算との結果として生じた6ビット・セグメントの2エンド・ビットが用いられて。Sボックス内の記憶専用記憶装置(ROM)に含まれる4個の16エントリー機能テーブルのうちの1つが選択される。各エントリーは4ビットから成つている。次に。選択された機能テーブルにおける16個の4ビット・エントリーのうちの1つが。供給された6ビット・セグメントの残り4ビットを解読することにより選択される。8個のSボックスは並列的なものである。従つて8個の独立した置換機能が実行されて。32ビットより成る1組の代替を決定する8個の4ビット・セグメントが与えられる。次いで。これらの32ビットはPボックス600において。更に決められた置換による置換置換を受ける。このような評価形変換及び加算操作の組合わせにより。メッセージ・ブロックの第1半分に対する32ビットの新ブロック暗号が生成される。この新ブロック暗号は。モジュロ2加算器650～664へ印加される。LDR250にあるメッセージ・ブロックの第2半分の32データ・ビットもモジュロ2加算器650～664へ印加される。モジュロ2加算器650～664は。メッセージ・ブロックの第1半分に対するPボックス600からの32ビットの新ブロック暗号に従つて。LDR250からのメッセージ・ブロックの残り32ビットを置換する。この結果。メッセージ・ブロ

ックの変更された第２半分を表わす新しい３２ビットの組を構成する８個の４ビット・グループが与えられる。メッセージ・ブロックの変更された第２半分の３２ビットは、メッセージ・ブロックの第１半分を含んでいたＵＤＲ２００へ印加される。これと同時に、メッセージ・ブロックの第１半分は、第２半分を含んでいたＬＤＲ２５０へ印加される。かくすることにより、メッセージ・ブロックの第１半分及び第２半分の互換が遂行される。

暗号化プロセスの次の繰返し時においては、ＵＫＲ５５０及びＬＫＲ４００に記憶されている暗号キーが、所定のシフト計画に従ってシフトされ、これにより新しい暗号キー・ビットの組が供給される。次に、ＵＤＲ２００に記憶されているメッセージ・ブロックの変更された第２半分の３２ビットが、同々な様ブロック暗号操作において、新しい暗号キー・ビットの組と共に使用される。モジュロ２加算器６５０～６６４は、この様ブロック暗号処理の結果に応じて、ＬＤＲ２５０に記憶されているメッセージ・ブロックの第１半分の３２ビットを変更する。この変更された第１半分の３２ビットは、メッセージ・ブロックの変更された第２半分の３２ビットを記憶していたＵＤＲ２００へ印加される。これと同時に、変更された第２半分の３２ビットは、メッセージ・ブロックの第１半分の３２ビットを記憶していたＬＤＲ２５０へ転送される。

最後の繰返しを除く後続の各繰返し操作時においては、ＵＫＲ５５０及びＬＫＲ４００にある暗号キー・ビットは、所定のシフト計画に従ってシフトされ、ＬＤＲ２５０に記憶されているメッセージ・ブロックの変更された半分（３２ビット）は、ＵＤＲ２００に記憶されているメッセージ・ブロックの前に変更された半分の３２ビットの様ブロック暗号に従って再変更され、そしてモジュロ２加算器６５０～６６４からの再変更された半分は、前に変更された他方の半分を記憶していたＵＤＲ２００へ印加され、これと同時に、この他方の半分はＬＤＲ２５０へ転送されて、メッセージ・ブロックの第１半分及び第２半分の互換が行なわれる。

最後の繰返し操作時には、ＵＫＲ５５０及びＬＫＲ４００にある暗号キー・ビットは、所定のシフト計画に従って最終シフトされて、解読された最後の暗号キー・ビットの組が生成され、ＬＤＲ２５０に記憶されている３２ビットの変更された半分に対する最後の再変更が、ＵＤＲ２００に記憶されている前に変更された半分の３２ビットの様ブロック暗号に従って実行される。しかしながら、モジュロ２加算器６５０～６６４からの前変更された半分及びＵＤＲ２００に記憶されている前に変更された半分は互いに交換されることはなく、元のメッセージ・ブロックに対する６４ビットの暗号化されたブロックを構成する。１６回目の繰返し後に、ＵＤＲ２００の３２ビットの内容及びモジュロ２加算器６５０～６６４の３２ビットの出力（これらは一緒になって、暗号化されたデータ・メッセージ・ブロックを表わす）は、上部出力バッファ（ＵＯＢ）７００及び下部出力バッファ（ＬＯＢ）７５０へ各々転送される。次いで、ＵＯＢ７００に記憶されている暗号化された４個の８ビット・バイトのデータ及びＬＯＢ７５０に記憶されている暗号化された４個の８ビット・バイトのデータで構成される６４ビットの暗号化されたデータ・ブロックは、８ビット・バイト単位の並列－直列変換を受け、一時に１バイトずつＰボックス８００へ与えられる。６４ビットの暗号化されたデータ・メッセージ・ブロックを完全に転送し終るためには、８サイクルが必要である。暗号化されたデータの各バイトは、受信局への伝送のために、暗号化されたデータ・ビットをデータ・バス・アウトの適切なビット線へ確実すべく、Ｐボックス８００において最後の順形置換を受ける。

受信局においては、同じ暗号キーの制御のもとに同様な１６回の繰返し操作を実行することにより、６４ビットの暗号化されたデータ・メッセージ・ブロックが解読される。しかしながら、暗号化プロセスの時とは異なり、解読プロセスに先立つＵＫＲ５５０及びＬＫＲ４００の暗号キー内容

の事前シフトは行なわれない。解読プロセスの繰返しなおく（初回のものを除く）においては、ＵＫＲ３５０及びＬＫＲ４００の暗号キー内容は、暗号化プロセスの時と同様に、所定のシフト計画に従つて、１又は２ビット位置だけシフトされるが、暗号化プロセスを逆にして、その時実行されたすべての繰返しを元に戻すため、暗号キーのシフト方向は暗号化プロセスの時とは反対にされる。かくすることにより、元の６４ビットのメッセージ・ブロックと同一のメッセージ・ブロックが再生される。また、解読プロセスの繰返し操作中に、ＵＫＲ３５０及びＬＫＲ４００の暗号キー内容は２７ビット位置シフトされる。従つて、ＵＫＲ３５０及びＬＫＲ４００は共に２８ビットのシフト・レジスタであるから、解読プロセスの終りにおいて、ＵＫＲ３５０及びＬＫＲ４００の暗号キー内容は、更に１ビット位置だけ単独シフトされる。この結果、暗号キーは所定のシフト計画に従つて、ＵＫＲ３５０及びＬＫＲ４００において完全に１回転シフトされることになり、解読プロセスの各繰返し操作における暗号キー・ビットの適切な整列を確実に行なわせると共に、別の解読プロセスに対する準備ができる。

本発明に従う暗号装置の詳細は第３ａ－３ｊ図に示されており、以下これらの図面並びに第７ａ図及び７ｂ図のタイミング図を参照して、より詳細な説明を行なうが、その前に、本発明の暗号装置で使用されるラッチ回路の具体例について、第４図を参照してお説明しておく。ラッチ回路１０は、４相のタイミング・クロックで動作されるダイナミックＦＥＴ回路によつて実現することができる。各クロック相は、例えば２５０ナノ秒の持続時間を有しており、この場合、完全な１クロック・サイクルは１マイクロ秒になる。基本ラッチ回路は、正電源と線２８との間に接続され、ゲート電極に繰返しクロック信号φ１が印加される素子２２と、線２８及び２９の間に並列的に接続され、各々のゲート電極に入力Ｄ３及びＧ３並びに入力Ｄ４及びＧ４が印加される２対の素子２３及び２４並びに２５及び２６と、線２９及び接地間に接続された、ゲート電極に繰返しクロック信号φ２が印加される素子３０と、正電源及び接地間に接続された、各々のゲート電極が繰返しクロック信号φ３、線２８及び繰返しクロック信号φ４に接続された３個の直列接続素子３２、３３及び３４とを有している。素子３２及び３３間の接続点は、ラッチ回路１０の出力線３６へ接続されると共に、素子２５のゲート電極へフィードバック接続されて、入力Ｄ４を与える。回路内の線遅キャパシタンス及び電極間キャパシタンスは、一まとめにしてキャパシタ３１及び３５として示されている。素子２３及び２４並びに２５及び２６はアンド回路として、線２８はドット・オア手段として、そして素子３３はインバータとして各々働く。

次に、第５図をも参照して、第４図のラッチ回路１０の動作について説明する。ラッチ回路１０が最初"０"状態にあるものとすると、クロック信号φ１が印加されて、素子２２がターン・オンされた時には、線２８は正電源の電位まで充電される。この時、クロック信号φ２は印加されていないので、素子３０はカット・オフ状態に保たれており、従つて線２８の充電は確実に行なわれる。次に、クロック信号φ２が印加されると、線２８上の電荷は、入力Ｄ３及びＧ３又は入力Ｄ４及びＧ４へ印加される信号次第にて、そのまま保たれるか又は放電される。ラッチ回路１０は０状態にあるものと仮定しているので、入力Ｄ４には低レベルの信号が印加されて、素子２５を非導通に保ち、また入力Ｇ４にも低レベルの信号が印加されて、素子２６を非導通に保つ。従つて、素子２５、２６及び３０を介する放電路は働かない。素子２３及び２４を含む放電路に関しては、もし入力Ｄ３に"１"ビット（高レベル信号）が印加され、且つこれと同時に入力Ｇ３にゲート信号（高レベル信号）が印加されると、素子２３及び２４は共に導通して、素子３０を介する放電路を形成し、その結果、線２８上の電荷は接地電位の方へ放電される。これに対し、入力Ｄ３に"０"ビット（低レベル信号）が印加されていると、たとえ入力Ｇ３にゲート信号が印加されても、クロックφ２

の間素子２３は非導通に保たれるので、線２８から素子２４及び３０を介して接地に至る放電路はあかず、従つてｈレベルの信号が線２８上に保持される。

次に、素子３２のゲート電極へクロック信号φ３が印加されると、この時はまだクロック信号φ４が印加されていないので、素子３４は非導通に保たれており、従つて線３６は正電源の電位まで充電される。次に、素子３４のゲート電極へクロック信号φ４が印加されると、線３６よりの電荷は、線２８上の信号のレベルに応じてそのまま保持されるか又は放電される。もし線２８上に"１"ビットのデータ入力を表わす低レベルの信号が存在すると、クロックφ４の間素子３３は非導通に保たれ、従つて線３６から素子３４を介して接地に至る放電路は働かず、線３６上には"１"ビットの存在を表わす高レベルの信号が保持される。入力Ｄ３に新しい入力信号が印加されない限り、ゲート信号Ｇ３は低レベルに、つゲート信号Ｇ４は高レベルに保たれるので、ラッチ回路１０が"１"ビット状態にセットされた後は、素子２５及び２６のゲートに高レベルの信号が印加され、従つて次のφ２クロック時に素子２５、２６及び３０を介する放電路が働いて、線２８を低レベルに与つ。これにより素子３３は非導通に保たれるので、素子３４を介する放電路は働かず、かくして線３６は、次の新しいデータ入力が印加されて、第５図に示されるようなゲート信号Ｇ３及びＧ４が印加されるまで高レベルに保たれる。これに対して、"０"ビットのデータ入力の結果として、線２８上に高レベルに信号が存在すると、クロックφ４の印加時に素子３３が導通して、素子３４を介する放電路を形成し、その結果、線３６上には"０"ビットの存在を表わす低レベルの信号が保持される。この場合、入力Ｄ４に低レベルの信号が印加されることになるので、素子２５は非導通に保たれ、従つて線２８に対する放電路は形成されない。このため、線２８上には電荷即ち高レベルの信号が保持される。この状態はまた素子３３を導通状態に保ち、これにより素子３４を介する放電路が

維持されて、線３６を低レベルに保つ。かくして、ラッチ回路１０の出力において所望データが確実に得られる。

ラッチ回路１０が"１"状態にある場合にも、クロック・サイクルは素子２２へのクロック信号φ１の印加によつて開始される。前と同様に、素子２２はクロックφ１の印加により導通して、線２８を正電源の電位まで充電させる。次に、クロック信号φ２が印加されると、線２８上の電荷は、入力Ｄ３及びＧ３又は入力Ｄ４及びＧ４に印加されている信号のレベルに応じて、そのまま保持されるか又は放電される。もし入力Ｄ３に"１"ビットのデータが印加されると、線２８上には低レベルの信号が保持され、一方入力Ｄ３に"０"ビットのデータが印加されると、高レベルの信号が保持される。次に、素子３２のゲート電極へクロック信号φ３が印加されると、この時クロック信号φ４がまだ印加されていないので、素子３４は非導通に保たれ、従つて、線３６は正電源の電位まで充電される。次に、素子３４のゲート電極へクロック信号φ４が印加されると、線３６上の電荷は、線２８上の信号のレベルに応じて、そのまま保持されるか又は放電される。前に説明したように、"１"ビットのデータ入力の結果として、線２８上に低レベルの信号が存在すると、線３６上には高レベルの信号が保持されて、"１"ビットの存在を表わし、一方、"０"ビットのデータ入力の結果として、線２８上に高レベルの信号が存在すると、線３６上には低レベルの信号が保持されて、"０"ビットの存在を表わす。

ラッチ回路１０は、入力Ｄ１及びＧ１に各々接続された素子１８及び１９を使用することによつて、２ウエイ入力へ拡張することができ、更に他の入力Ｄ２及びＧ２に各々接続された素子２０及び２１を使用することによつて、３ウエイ入力へ拡張することもできる。以下で詳細に説明する本発明の実施例においては、１ウエイ入力、２ウエイ入力又は３ウエイ入力のラッチ回路が必要に応じて使用される。

まず第３０図に示されるように、８バイトから

成る６４ビットのデータ・メッセージ・ブロックは、データ・バス・インを介して一時に１バイトずつＰボックス５０へ印加される。各バイトはＰボックス５０において初期置換を受け、偶数番目（０、２、４、６）のデータ・ビットより成る組及び奇数番目（１、３、５、７）のデータ・ビットより成る組に分割される。偶数番目の組はＵＩＢ１００へ送られ、一方、奇数番目の組はＬＩＢ１５０へ送られる。ＵＩＢ１００は４個の８段シフト・レジスタ０ＵＩＢ、１ＵＩＢ、２ＵＩＢ及び３ＵＩＢで構成され、ＬＩＢ１５０も同様に４個の８段シフト・レジスタ０ＬＩＢ、１ＬＩＢ、２ＬＩＢ及び３ＬＩＢで構成される。第３ａ図には、第１シフト・レジスタ０ＵＩＢの最初及び最後の段のみが詳細に示されているが、他のシフト・レジスタもこれと同じ構成である。

第７ａ図のタイミング図をも併せて参照するに、サイクル０において、１つの有効データ・バイトがＰボックス５０を介して、ＵＩＢ１００及びＬＩＢ１５０へ印加されている時に、タイミング及び制御論理６０からＬＩＢ（Ｇ３）線及び$\overline{\text{ＬＩＢ}}$（Ｇ４）線へ信号が印加されて、最初の８ビット・バイトが、ＵＩＢ１００及びＬＩＢ１５０の各シフト・レジスタの最初の段のラッチ（例えば１０２）へロードされる。メッセージ・ブロックの残りの８ビット・バイトは、後続のサイクル１から７までの間に、一時に１バイトずつＵＩＢ１００及びＬＩＢ１５０へ印加される。この場合、バイトの各ビットは、各シフト・レジスタの最初の段（Ｄ３）へ印加される。ＬＩＢ線及び$\overline{\text{ＬＩＢ}}$線上の信号は、シフト・レジスタの各段へ印加されるので、サイクル１乃至７の各々において、データ・ビットは各シフト・レジスタ内で１ビット位置ずつシフト・ダウンされ、従ってサイクル７の終了時には、ＵＩＢ１００及びＬＩＢ１５０は、供給されたデータ・メッセージ・ブロックを半分ずつロードされている。ＵＩＢ１００及びＬＩＢ１５０は直列－並列変換を実行し、その結果、ＵＩＢ１００及びＬＩＢ１５０へ逐次に供給された８バイトのメッセージ・ブロックは、これらの出力において、各々３２ビットより成る２つのグループ（メッセージ・ブロックの第１半分及び第２半分）へ転成される。

次いで、第３ｂ、３ｃ及び３ｄ図を参照するに、６４ビットのメッセージ・ブロックがＵＩＢ１００及びＬＩＢ１５０へ受取られて、そこにパンファされている間に、６４ビットの外部レジスタからキー・バス・インを介して、暗号キーが一時に７ビット・バイトずつＰボックス３００へ逐次に印加される。各７ビット・バイトはＰボックス３００で初期置換を受け、最初の４キー・ビット及び残りの３キー・ビットへ分割される。最初の４キー・ビットはＵＫＲ３５０へ印加され、一方、残りの３キー・ビットはビット位置を逆にしてＬＫＲ４００へ印加される。ＵＫＲ３５０は５個の８段シフト・レジスタ０ＵＫＲ、１ＵＫＲ及び２ＵＫＲ並びに１個の４段シフト・レジスタ３ＵＫＲで構成され、同様にＫＲ４００も３個の８段シフト・レジスタ０ＬＫＲ、１ＬＫＲ及び２ＬＫＲ並びに１個の４段シフト・レジスタ３ＬＫＲで構成される。シフト・レジスタ３ＵＫＲの４段目のラッチ３９０の出力は、シフト・レジスタ３ＬＫＲの１段目のラッチ４０２の入力に接続されている。第３ｄ図に詳細に示されているように、８段シフト・レジスタ０ＵＫＲの第１段は３ウエイ入力ラッチ３５２で構成され、他の段は第２段及び最後の段のラッチ３５４及び３５６の如き２ウエイ入力ラッチで構成される。８段シフト・レジスタ１ＵＫＲ及び２ＵＫＲもこれと同じ構成である。４段シフト・レジスタ３ＵＫＲについては、第３ｅ図に示されるように、第１段は３ウエイ入力ラッチ３８４で構成され、他の各段はラッチ３９０の如き２ウエイ入力ラッチで構成される。第３ｅ及び３ｄ図にブロック図で簡単に示されているＬＫＲ４００の８段シフト・レジスタ０ＬＫＲ、１ＬＫＲ及び２ＬＫＲは、ＵＫＲ３５０の対応する８段シフト・レジスタ０ＵＫＲ、１ＵＫＲ及び２ＵＫＲと同じ構成を有している。第３ｄ図に示される４段シフト・レジスタ３ＬＫＲについては、その第１段は、シフト・レジスタ３ＵＫＲの最終

段のラッチ390の出力に接続された3ウエイ入力ラッチ402で構成され、他の各段は最終段のラッチ408の如き2ウエイ入力ラッチで構成される。かくして、UKR350及びLKR400の組合わせは、暗号キー・ワードのキー・ビットを記憶するための7個の8段シフト・レジスタから成つているものと考えることができる。

次に、第7a図を参照して、暗号キーのロード動作について説明する。サイクル0において有効暗号キー・バイトがPボックス300を介してUKR350及びLKR400へ印加される時に、シフト・レジスタ0UKR、1UKR、2UKR、3UKR、0LKR、1LKR及び2LKRの第1段に接続されたLDK(G3)線及び$\overline{LDK}$(G4)線へ信号が印加され、これにより最初の7ビット・キー・バイトがUKR350及びLKR400の7個の各シフト・レジスタの第1段、例えば入力ラッチ552、568及び384などへロードされる。

サイクル1においては、暗号キーの2番目の7ビット・バイトが、UKR350及びLKR400の7個のシフト・レジスタの第1段へロードされる。これと同時に、各第1段の以前の内容即ち暗号キーの最初の7ビット・バイトは、シフト・レジスタ0UKR、1UKR、2UKR、3UKR、0LKR、1LKR及び2LKRの第2段に接続されているSR(G3)線及び$\overline{LDK}$線への信号印加により、各々1ビット位置だけシフト・ダウンされる。各段のラッチ内部の分解時間(resolving time)は、前段のラッチの出力に変化が生じる前にシフト動作を行なわせるのに十分なものである。

サイクル2においては、暗号キーの3番目の7ビット・バイトが、UKR350及びLKR400の7個のシフト・レジスタの第1段へロードされる。これと同時に、第1段及び第2段の以前の内容即ち暗号キーの2番目及び最初の7ビット・バイトは、シフト・レジスタ0UKR、1UKR、2UKR、3UKR、0LKR、1LKR及び2LKRの第2段及び第3段に接続されているSR線及び$\overline{LDK}$線への信号印加により、各々1ビット位置だけシフト・ダウンされる。

サイクル3及び4においては、暗号キーの4番目及び5番目の7ビット・バイトが、7個のシフト・レジスタの第1段へ逐次にロードされ、これと同時にその内容は1ビット位置ずつシフト・ダウンされる。しかしながら、シフト・レジスタ3UKRの最終段にあるビットは、サイクル4においてシフト・レジスタ3LKRの第1段へシフトされる。最後のサイクル5、6及び7においては、暗号キーの残りの7ビット・バイトが、シフト・レジスタ0UKR、1UKR、2UKR、3UKR、0LKR及び2LKRの第1段へ一時に1バイトずつロードされる。LDK線及び$\overline{LDK}$線上の信号は、各シフト・レジスタの第1段へ印加され、一方、SR線及び$\overline{LDK}$線上の信号は、各シフト・レジスタの残りの段へ印加されるので、サイクル5、6及び7の各々においては、暗号キー・ビットは1ビット位置ずつシフト・ダウンされ、従つてサイクル7の終了時には、UKR350及びLKR400は暗号キーの第1半分及び第2半分を各々ロードされている。

暗号キーのロード動作においては、UKR350及びLKR400は直列-並列変換を行ない、従つてUKR350及びLKR400に記憶されている暗号キーの8個の7ビット・バイトは、各々28ビットより成る2組の並列グループとして考えることができる。下記の表1及び表2は、UKR350及びLKR400へ暗号キーをロードする際のキー・ビットのマッピングの様子を示したものである。

表　1

UKRに対する暗号キーのマップ

UKRのビット位置	暗号キー・ビット							
UKR 0 - UKR 7	56	48	40	32	24	16	8	0
UKR 8 - UKR 15	57	49	41	33	25	17	9	1
UKR 16 - UKR 23	58	50	42	34	26	18	10	2
UKR 24 - UKR 27	59	51	43	35				

表　2

LKRに対する暗号キーのマップ

LKRのビット位置	暗号キー・ビット							
LKR 0 - LKR 7	62	54	46	38	30	22	14	6
LKR 8 - LKR 15	61	53	45	37	29	21	13	5
LKR 16 - LKR 23	60	52	44	36	28	20	12	4
LKR 24 - LKR 27	27	19	11	3				

第３ａ図に示されるＵＤＲ２００及びＬＤＲ２５０は、各々３２段のラッチＯＵＤＲ～３１ＵＤＲ及びＯＬＤＲ～３１ＬＤＲで構成される。第７ａ図に示されるように、マイクル８において１Ｂ下線及びＬＤＲ線へ信号が印加され、これによりＵＩＢ１００にある３２個のデータ・ビット及びＬＩＢ１５０にある３２個のデータ・ビットが、各々ＵＤＲ２００及びＬＤＲ２５０へ並列的に転送される。メッセージ・ブロックの６４ビットは、下記の表３及び表４に示されるごとく、ＵＤＲ２００及びＬＤＲ２５０へ分配される。

表　3

UDRに対するデータのマップ

UDRのビット位置	データ・ビット							
UDR 0 - UDR 7	56	48	40	32	24	16	8	0
UDR 8 - UDR 15	58	50	42	34	26	18	10	2
UDR 16 - UDR 23	60	52	44	36	28	20	12	4
UDR 24 - UDR 31	62	54	46	38	30	22	14	6

表　4

LDRに対するデータのマップ

LDRのビット位置	データ・ビット							
LDR 0 - LDR 7	57	49	41	33	25	17	9	1
LDR 8 - LDR 15	59	51	43	35	27	19	11	3
LDR 16 - LDR 23	61	53	45	37	29	21	13	5
LDR 24 - LDR 31	63	55	47	39	31	23	15	7

第７ａ図に示されるように、ＬＤＫ制御信号以上信号は印加されない。従って、シフト・レジスタ３ＵＫＲの最終段のラッチ３９０からシフト・レジスタ３ＬＫＲの第１段のラッチ４０２に至る帰還は以後使用されず、これらの間では何なるビット転送も行なわれない。シフト・レジスタ３ＵＫＲの最終段のラッチ３９０の出力は、シフト・レジスタＯＵＫＲの第１段のラッチ３５２に転送され、シフト・レジスタ３ＬＫＲの最終段のラッチ４０８の出力は、シフト・レジスタＯＬＫＲの第１段のラッチ（図示せず）に帰還されているので、ＵＫＲ３５０及びＬＫＲ４００は、各々独立した２８ビットのシフト・レジスタと考えることができる。ＵＫＲ３５０及びＬＫＲ４００に記憶されている暗号キー・ビットは、暗号化プロセスに先立つて１ビット位置ずつ巡回シフト・アップされる。この場合、ＵＫＲ３５０の第１段のラッチ３５２に記憶されていたビットは、ＵＫＲ３５０の最終段のラッチ３９０へ循環シフトされ、同様に、ＬＫＲ４００の第１段のラッチに記憶さ

れていたビットは、ＬＫＲ４００の最終段のラッチ４０８へ循環シフトされる。このような準前シフトは、サイクル８において、ＵＫＲ３５０及びＬＫＲ４００のすべての段に印加されているＳＬ及び$\overline{\text{ＬＤＫ}}$への信号を印加することにより行なわれる。各ラッチの出力は前段のラッチへ接続されており、従つて、ＳＬ線及び$\overline{\text{ＬＤＫ}}$線への信号印加により、各ラッチから前段のラッチへキー・ビットが転送される。例えば、これらの信号印加によつてラッチ３５４のビット内容をラッチ３５２へ有効にシフトさせるため、ラッチ３５４の出力ＵＫＲ１はラッチ３５２の１入力に接続されている。同様に、ラッチ３５２のビット内容をラッチ３９０へ有効にシフトさせるため、ラッチ３５２の出力ＵＫＲ０はラッチ５９０の１入力に接続されている。暗号化プロセスの開始前に行なわれるこのような暗号キー・ビットの準前シフトは、暗号化プロセスの最初の繰返しにおけるキー・ビットの適切な整列を確実にするものである。暗号化プロセスに入ると、ＵＫＲ３５０及びＬＫＲ４００にある暗号キー・ビットを更に２７ビット位ずつシフトさせるため、最初の繰返しを除く各繰返しの間に、ＵＫＲ３５０及びＬＫＲ４００は１又は２ビット位置ずつシフト　ナップされる。ＵＫＲ３５０及びＬＫＲ４００は共に２８ビットのシフト・レジスタであるから、これらに記憶されている暗号キー・ビットの２８シフト、即ち、１準前シフト及び暗号化プロセスにおける２７シフトは、暗号化プロセスの開始時と同様、繰返し動作のために暗号キー・ビットを適切に整列させるものである。下記の表５は、暗号キーに対する所定のシフト計画を示したものである。

表　５

暗号キーのシフト計画

繰返し番号	（準前シフト）	暗号化（シフト・アップ）	復号（シフト・ダウン）
	1		
1		1	1
2		2	2
3		2	2
4		2	2
5		2	2
6		2	2
7		2	2
8		1	1
9		2	2
10		2	2
11		2	2
12		2	2
13		2	2
14		2	2
15		1	1
16		（準前シフト）	1

れていたビットは、ＬＫＲ４００の最終段のラッチ４０８へ循環シフトされる。このような事前シフトは、サイクル８において、ＵＫＲ５５０及びＬＫＲ４００のすべての段にセットされているＳＬ線及び$\overline{\text{ＬＤＫ}}$線へ信号を印加することにより行なわれる。各ラッチの出力は前段のラッチへ接続されており、従って、ＳＬ線及び$\overline{\text{ＬＤＫ}}$線への信号印加により、各ラッチから前段のラッチへキー・ビットが転送される。例えば、これらの信号印加によってラッチ３５４のビット内容をラッチ３５２へ有効にシフトさせるため、ラッチ３５４の出力ＵＫＲ１はラッチ３５２の１入力に接続されている。同様に、ラッチ３５２のビット内容をラッチ３９０へ有効にシフトさせるため、ラッチ３５２の出力ＵＫＲ０はラッチ３９０の１入力に接続されている。暗号化プロセスの開始前に行なわれるこのような暗号キー・ビットの事前シフトは、暗号化プロセスの最初の繰返しにおけるキー・ビットの適切な整列を確実にするものである。暗号化プロセスに入ると、ＵＫＲ５５０及びＬＫＲ４００にある暗号キー・ビットを次に２７ビット位シフトさせるため、最初の繰返しを除く各繰返しの間に、ＵＫＲ５５０及びＬＫＲ４００は１又は２ビット位置ずつシフト・アップされる。ＵＫＲ５５０及びＬＫＲ４００は共に２８ビットのシフト・レジスタであるから、これらに記憶されている暗号キー・ビットの２８シフト、即ち、１事前シフト及び暗号化プロセスにおける２７シフトは、暗号化プロセスの開始時と同様、繰返し操作の間に暗号キー・ビットを適切に整列させるものである。下記の表５は、暗号キーに対する所定のシフト計画を示したものである。

表　5

暗号キーのシフト計画

繰返し番号	暗号化（シフト・アップ）〈事前シフト〉	新鍵（シフト・ダウン）
	1	
1	1	1
2	2	2
3	2	2
4	2	2
5	2	2
6	2	2
7	2	2
8	1	1
9	2	2
10	2	2
11	2	2
12	2	2
13	2	2
14	2	2
15	1	1
16	〈事後シフト〉 1	1

表5中の"1"は、UKR350及びLKR400における1ビット位置のシフトを表わし、"2"は2ビット位置のシフトを表わす。

暗号化プロセス

本発明に従う暗号装置を使用する暗号化プロセスは、16回の繰返し操作によって、データ・ビットのメッセージ・ブロックを暗号化する。

UKR350及びLKR400にある暗号キー・ビットの巡回シフトは、暗号化プロセスの開始前に、サイクル8において実行される。これは、UKR350及びLKR400のすべての段に印加されているSL線及び$\overline{\text{LDK}}$線へ最初の信号を印加することによって行なわれ、暗号キーは1ビット位置だけシフト・アップされる。この結果、サイクル8の終了時には暗号化プロセスの最初の繰返し操作のための暗号キー・ビットの最初の組が与えられる。暗号化プロセスの最初の繰返し操作は、サイクル9及び10で実行され、UKR550にある28個の巡回シフトされた暗号キー・ビットのうちの24ビット及びLKR400にある28個の巡回シフトされた暗号キー・ビットのうちの24ビットをPボックス450で置換することにより開始される。Pボックス450は、下記の暗号キー・ビットのマッピングを示す表6及び7に従って、UKR350及びLKR400からの48ビットの任意に決められた順序を行なう。

表 6

暗号キー・ビットの置換マップ

ビット番号	置換されたビット番号
UKR 0	UKR 13
UKR 1	UKR 16
UKR 2	UKR 10
UKR 3	UKR 23
UKR 4	UKR 0
UKR 5	UKR 4
UKR 6	UKR 2
UKR 7	UKR 27
UKR 9	UKR 14
UKR 10	UKR 5
UKR 11	UKR 20
UKR 12	UKR 9
UKR 13	UKR 22
UKR 14	UKR 18
UKR 15	UKR 11
UKR 16	UKR 3
UKR 18	UKR 25
UKR 19	UKR 7
UKR 20	UKR 15
UKR 22	UKR 6
UKR 23	UKR 26
UKR 25	UKR 19
UKR 26	UKR 12
UKR 27	UKR 1

表 7

暗号キー・ビットの置換マップ

ビット番号	置換されたビット番号
LKR 0	LKR 12
LKR 1	LKR 23
LKR 2	LKR 2
LKR 3	LKR 8
LKR 4	LKR 18
LKR 5	LKR 26
LKR 7	LKR 1
LKR 8	LKR 11
LKR 10	LKR 22
LKR 11	LKR 16
LKR 12	LKR 4
LKR 13	LKR 19
LKR 15	LKR 15
LKR 16	LKR 20
LKR 17	LKR 10
LKR 18	LKR 27
LKR 19	LKR 5
LKR 20	LKR 24
LKR 21	LKR 17
LKR 22	LKR 13
LKR 23	LKR 21
LKR 24	LKR 7
LKR 26	LKR 0
LKR 27	LKR 3

8個の6ビット・セグメントと考えられる48個の置換された暗号キー・ビットは、各々6個の排他的オア回路（第3c、5f及び3g図にXORで示されている）より成る8個のモジュロ2加算器500、502、504、506、508、510、512及び514へ1入力として印加される。これと同時に、UDR200に含まれる32データ・ビットより取り出つ8個の4ビット・セグメントと考えられるメッセージ・ブロックの第1半分が、8個の6ビット・セグメントを構成する48個のデータ・ビットへ拡張されて、8個のモジュロ2加算器500～514の他の入力へ印加される。データ・ビットの拡張は、第3c、5f及び3g図に示されるように、8個の4ビット・セグメントの各々のエンド・ビット（図示の例では、各4ビット・セグメントの最初の2ビット）を二重にすることによつて達成される。下記の表8及び表9に示されるように、8個のモジュロ2加算器500～514は、拡張された48個のデータ・ビット及び置換された48個の暗号キー・ビットを結合わせて、8個の8ボックス内ちオアフィン変換機能ボックス502～564に対する選ばの引数を構成する新しい8個の6ビット・セグメント変出力する。

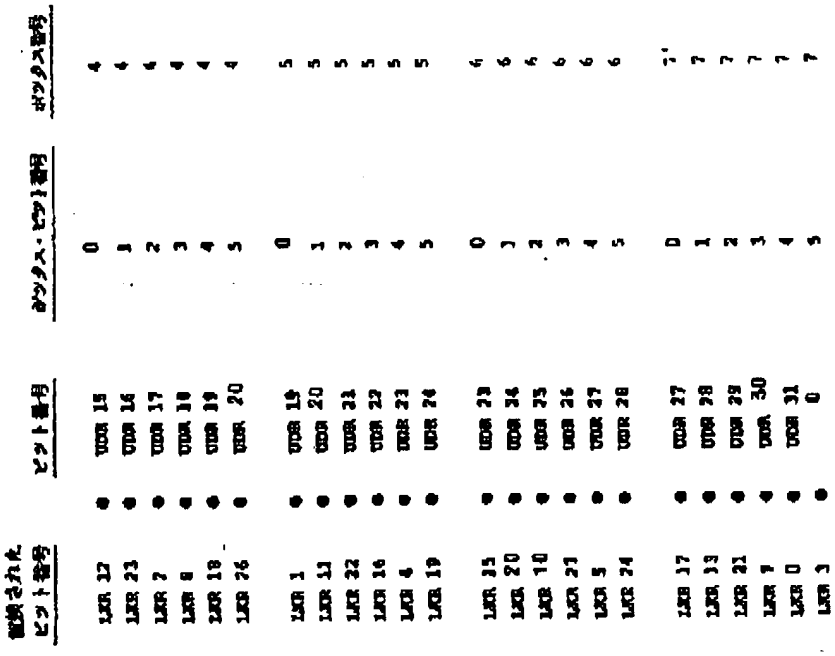
表 6

ボックスのマッピング計画

置換されたビット番号	ビット番号	ボックス・ビット番号	ボックス番号
32 13	32	0	0
1 34	1	1	0
2 10	2	2	0
3 23	3	3	0
4 0	4	4	0
5 4	5	5	0
6 3	6	0	1
7 27	7	1	1
8 14	8	2	1
9 5	9	3	1
10 20	10	4	1
11 9	11	5	1
12 22	12	0	2
13 18	13	1	2
14 11	14	2	2
15 3	15	3	2
16 25	16	4	2
17 7	17	5	2
18 15	18	0	3
19 6	19	1	3
20 26	20	2	3
21 19	21	3	3
22 12	22	4	3
23 1	23	5	3

第 9

ボックスのマッピング計画



第３図中の＃０９ボックス５５０の計画を第６図に示す。図示の如く、＃０９ボックス５５０はデコーダ５５２及びＲＯＳ５８４から成つている。この＃０９ボックス５５０へは、＃０モジュロ２加算器５５０からの６ビット・セグメントが入力として印加される。この６ビット・セグメントのエンド・ビット０及び５、即ち、二重にされたデータ・ビットＵＤＲ３１及び重畳された暗号キー・ビットＵＫＲ１３のモジュロ２加算と、二重にされたデータ・ビットＵＤＲ４及び重畳された暗号キー・ビットＵＫＲ４のモジュロ２加算とから生成されたビットを表わす信号は、インバータ５５４及び５５６へ各々印加され、これによりエンド・ビットの補数信号が得られる。エンド・ビットのモジュロ２加算の結果が００であれば、各々１６個のアンド回路を含む４グループのうちの１つ、即ち、アンド回路５６８及び５７０を含む第１グループが選択される。同様に、エンド・ビットのモジュロ２加算の結果が０１であれば、アンド回路５７２及び５７４を含む第２グループが選択され、結果が１０であれば、アンド回路５７６及び５７８を含む第３グループが選択され、そして最後に結果が１１であれば、アンド回路５８０及び５８２を含む第４グループが選択される。＃０８ボックス５５０へ印加される６ビット・セグメントの内側の４ビット（１、２、３、４）を表わす信号は、対応するインバータ５５８、５６０、５６２及び５６４へ各々印加され、これにより内側４ビットの補数信号が生成される。６ビット・セグメントの内側４ビットは、選択されたグループに含まれる１６個のアンド回路のうちの１つによつて識別され、ＲＯＳ５８４の特定のアドレス動へ出力信号を送る。ＲＯＳ５８４は、基本的には４個の機能テーブル即ち０ＲＯＳ、１ＲＯＳ、２ＲＯＳ及び３ＲＯＳで構成される。各機能テーブルは、１６個のエントリーを有しており、これらの各エントリーは、素子５８６、５８７、５８８及び５８９の如き４個のＰＢＴ素子で実現され得る４ビットから成つている。これらの素子は、一旦選択されると、ＲＯＳ５８４の出力線５

594、595、596及び597へ一致的な4ビット・セグメントを供給する。この4ビット・セグメントは、Bボックス550の4本の出力線90、91、92及び93の方へ送られる。

※3～※8に示される他の7個のBボックス552、554、556、558、560、562及び564も、基本的には808ボックス550と同様な仕方でなっており、各Bボックスにはそれら個別テーブルは互いに異なつており、従つて8通りの異なつた変換機能が与えられる。下記の表10、11、12及び13は、8個のBボックス(※0～※7)の個別テーブルの出力を示すもので、各出力を表わす10進数は、実際には4ビットの2進パターン(例えば14→1110など)で出力される。

表 10

Bボックス個別テーブルA

Bボックスの入力ビット	※0Bボックス Bボックスのエンド・ビット 00 (0)	01 (1)	10 (2)	11 (3)	※1Bボックス Bボックスのエンド・ビット 00 (0)	01 (1)	10 (2)	11 (3)
0000 (0)	14	0	4	15	15	3	0	13
0001 (1)	4	15	1	12	1	13	14	8
0010 (2)	13	7	14	9	8	4	7	10
0011 (3)	1	4	8	2	14	7	11	1
0100 (4)	3	14	13	4	6	15	10	3
0101 (5)	15	2	6	9	11	2	4	15
0110 (6)	11	13	2	1	3	8	13	6
0111 (7)	8	1	11	7	4	14	1	2
1000 (8)	3	10	15	5	9	12	5	11
1001 (9)	10	6	12	11	7	0	8	6
1010 (10)	6	12	9	3	2	1	12	7
1011 (11)	12	11	7	14	13	10	6	12
1100 (12)	5	9	3	10	12	6	9	0
1101 (13)	9	5	10	0	0	9	3	5
1110 (14)	0	3	5	8	5	11	2	14
1111 (15)	7	8	0	13	10	5	15	9

表 11

Bボックス個別テーブルB

Bボックスの入力ビット	※2Bボックス Bボックスのエンド・ビット 00 (0)	01 (1)	10 (2)	11 (3)	※3Bボックス Bボックスのエンド・ビット 00 (0)	01 (1)	10 (2)	11 (3)
0000 (0)	10	13	11	1	7	13	10	3
0001 (1)	0	7	6	10	13	8	6	15
0010 (2)	9	0	4	15	14	11	9	0
0011 (3)	14	9	8	6	3	5	0	6
0100 (4)	6	3	8	6	0	6	12	10
0101 (5)	3	4	15	9	6	15	11	1
0110 (6)	15	6	3	8	9	0	7	13
0111 (7)	5	10	0	7	10	3	13	8
1000 (8)	1	2	11	4	1	4	15	9
1001 (9)	13	8	1	15	2	7	1	4
1010 (10)	12	5	2	14	8	2	3	5
1011 (11)	7	14	12	3	5	12	14	11
1100 (12)	11	12	5	11	11	1	5	2
1101 (13)	4	11	10	5	12	10	2	7
1110 (14)	2	15	14	2	4	14	8	12
1111 (15)	8	1	7	12	15	9	4	14

表　12

Sボックス検証テーブルC

Sボックスの内部ビット	#4Sボックス Sボックスのエンド・ビット 00 (0)	01 (1)	10 (2)	11 (3)	#5Sボックス Sボックスのエンド・ビット 00 (0)	01 (1)	10 (2)	11 (3)
0000 (0)	2	14	4	11	12	10	9	4
0001 (1)	12	11	2	8	1	15	14	3
0010 (2)	4	2	1	12	10	4	15	2
0011 (3)	1	12	11	7	15	2	5	12
0100 (4)	7	4	10	1	9	7	2	9
0101 (5)	10	7	13	14	2	12	8	5
0110 (6)	11	13	7	2	6	9	12	15
0111 (7)	6	1	8	13	9	5	3	10
1000 (8)	8	5	15	6	0	6	7	11
1001 (9)	5	0	9	15	13	1	0	14
1010 (10)	3	15	12	0	8	13	4	1
1011 (11)	15	10	5	9	4	14	10	7
1100 (12)	13	3	6	10	14	0	1	6
1101 (13)	0	9	3	4	7	11	13	0
1110 (14)	14	8	0	5	5	3	11	8
1111 (15)	9	6	14	3	11	8	6	13

表　13

Sボックス検証テーブルD

Sボックスの内部ビット	#6Sボックス Sボックスのエンド・ビット 00 (0)	01 (1)	10 (2)	11 (3)	#7Sボックス Sボックスのエンド・ビット 00 (0)	01 (1)	10 (2)	11 (3)
0000 (0)	4	13	1	6	13	1	7	2
0001 (1)	11	0	4	11	2	15	11	1
0010 (2)	2	11	13	13	8	13	4	14
0011 (3)	14	7	11	8	4	8	1	7
0100 (4)	15	4	12	1	6	10	9	4
0101 (5)	0	9	3	4	15	3	12	10
0110 (6)	8	1	7	10	11	7	14	8
0111 (7)	13	10	14	7	1	4	2	13
1000 (8)	3	14	10	9	10	12	0	15
1001 (9)	12	3	15	5	9	5	6	12
1010 (10)	9	5	6	0	3	6	10	9
1011 (11)	7	12	8	12	14	11	13	0
1100 (12)	5	2	0	14	5	0	15	3
1101 (13)	10	15	5	2	0	14	3	5
1110 (14)	6	8	9	3	12	9	5	6
1111 (15)	1	6	2	12	7	2	8	11

特開昭 64-51— 108701(19)

8個のSボックス550～564は、52ビットの代替グループを規定する8個の4ビット・セグメントを供給し、次いでこれらのセグメントは、Pボックス600において、任意に決められた順序によつて順列変換される。Sボックス550～564で実行される非線形変換及びPボックス600で実行される順列変換の結果、メッセージ・ブロックの第1半分の次ブロック暗号が生成される。下記の表14は、Sボックスの出力の順列置換の様子を示したものである。

表 14

Sボックス出力の置換マップ

Sボックス・ビット番号	置換されたビット番号
30	58
31	816
32	822
33	830
34	512
35	527
36	81
37	817
38	823
39	815
310	829
311	85
312	825
313	519
314	55
315	56
316	87
317	813
318	824
319	82
320	53
321	528
322	810
323	816
324	521
325	811
326	823
327	86
328	84
329	826
330	814
331	870

第3h、5i及び3j図に示されるように、別の8個のモジュロ2加算器650、652、654、656、658、660、662及び664は、各々4個の排他的オア回路XORで構成される。LDR250に保持されているメッセージ・ブロックの第2半分（32データ・ビットより成り、8個の4ビット・データ・セグメントと考えられる）は、メッセージ・ブロックの第1半分の対応ブロック暗号を表わす置換された32ビットのグループと共に、これらのモジュロ2加算器650～664の入力へ印加される。モジュロ2加算器650～664は、これらの入力から、メッセージ・ブロックの変更された第2半分を表わす新しい32ビットのグループを構成する8個の4ビット・セグメントを生成し、次いでこの新しい32ビットのグループは、母線を介して第3a図のUDR200へ転送される。

再び第3a図及び第7a図を参照するに、サイクル10の前半において、UDR200のすべてのラッチに接続されているLB線及びLDR線へ信号が印加され、これによりメッセージ・ブロックの変更された第2半分を表わす32ビットのグループがUDR200へロードされる。これと同時に、LB線及びLDR線上の信号は、LDR250のすべてのラッチへも印加され、この結果、UDR200に記憶されていたメッセージ・ブロックの第1半分がLDR250のラッチへ転送されて、そこに記憶される。メッセージ・ブロックの第1半分及び変更された第2半分のこのような互換は、暗号化プロセスの次の繰返し操作を実行するための準備であり、これで、サイクル8における暗号キーの事前シフト後に開始された最初の繰返し操作が完了したことになる。

2回目の繰返し操作は、サイクル10、11及び12で実行され、サイクル10におけるシフト動作から開始される。最初のサイクル10の間に、SL線及びLDK線を介してUKR350及びLKR400のすべての段へ印加される第2信号により、暗号キーが更に1ビット位置だけシフト・アップされる。これは、暗号化プロセスの2回目の繰返し操作に対する第2組の暗号キー・ビットをもたらすものである。サイクル11においては、UDR200に記憶されているメッセージ・ブロックの変更された第2半分が、上述と同様な仕方でブロック暗号処理操作で使用され、次にその結果がモジュロ2加算器650～664で使用されて、LDR250に記憶されているメッセージ・ブロックの第1半分が変更される。

サイクル12においては、UDR200のすべてのラッチに接続されているLB線及びLDR線への第2信号の印加により、メッセージ・ブロックの変更された第1半分を表わす新しい32ビットのグループがUDR200に記憶される。これと同時に、LB線及びLDR線上の第2信号は、LDR250のすべてのラッチへも印加され、これによりUDR200に記憶されていたメッセージ・ブロックの変更された第2半分がLDR250へ転送されて、そこに記憶される。この互換操作は、暗号化プロセスの次の繰返しを実行するための準備であり、これで暗号化プロセスの2回目の繰返し操作が完了される。

前記の表5の暗号キー・シフト計画に示されるように、暗号化プロセスの3回目の繰返し操作（サイクル11、12、13及び14で実行される）においては、暗号キーは2ビット位置だけシフトされねばならない。従つて、サイクル11の間にSL線及びLDK線へ第3信号を印加することにより、暗号キーの2回のシフトのうちの最初のシフトが行なわれる。3回目の繰返し操作を実行するためのこの最初のシフト動作は、暗号装置内の分解時間の故に、SL線への第2信号の印加によつて開始された2回目の繰返し操作に対して影響を及ぼさない。暗号キーは、サイクル12の間にSL線及びLDK線へ印加される第4信号によつて、更に1ビット位置だけシフト・アップされる。このように、暗号キーは、3回目の繰返し操作の間にSL線及びLDK線へ印加される第3信号及び第4信号により、2ビット位置だけシフト・アップされる。

暗号化プロセスにおける後続の繰返し操作も、

同様にしてまた暗号キーのシフト計画に従つて実行される。最後の繰返し操作を除く残りの各繰返し操作においては、ＵＫＲ３５０及びＬＫＲ４００に記憶されている暗号キー・ビットは、所定のシフト計画に従つてシフトされ、ＬＤＲ２５０に記憶されているメッセージ・ブロックの変更された半分は、ＵＤＲ２００に記憶されているメッセージ・ブロックの以前に変更された半分の被ブロック暗号に従つて再変更され、そしてモジュロ２加算器６５０～６６４からのこの再変更された半分は、メッセージ・ブロックの以前に変更された半分に代つてＵＤＲ２００へロードされ、これと同時に、ＵＤＲ２００に記憶されていたこの以前に変更された半分は、ＬＤＲ２５０へ転送されて、その前の内容に代つてそこに記憶される。

サイクル３８及び３９で実行される暗号化プロセスの最後の繰返し操作においては、ＵＫＲ３５０及びＬＫＲ４００に記憶されている暗号キー・ビットは、所定のシフト計画に従つて最終シフトされ、そしてＬＤＲ２５０に記憶されているメッセージ・ブロックの変更された半分に対する最後の再変更が、ＵＤＲ２００に記憶されているメッセージ・ブロックの以前に変更された半分の被ブロック暗号に従つて実行される。しかしながら、サイクル３９以降は、ＬＢ線上に信号が存在しないので、モジュロ２加算器６５０～６６４からの再変更された半分及びＵＤＲ２００に記憶されている以前に変更された半分は互換されず、これらは元のメッセージ・ブロックの被暗号化ブロックを構成する。かくして、６４ビットの被暗号化メッセージ・ブロックを表わすＵＤＲ２００からの３２ビットの出力及びモジュロ２加算器６５０～６６４からの３２ビットの出力は、対応するＵＯＢ７００及びＬＯＢ７５０へ各々印加される。第３ｈ、３ｉ及び３ｊ図に示されるように、ＵＯＢ７００は４個の８段シフト・レジスタ０ＵＯＢ、１ＵＯＢ、２ＵＯＢ及び３ＵＯＢで構成され、同様に、ＬＯＢ７５０も４個の８段シフト・レジスタ０ＬＯＢ、１ＬＯＢ、２ＬＯＢ及び３ＬＯＢで構成される。図面には、最初のシフト・レジスタ０ＵＯＢの第１段（ラッチ７０２）、第２段（ラッチ７０４）及び最終段（ラッチ７１６）のみが詳細に示されているが、残りの段及び他のシフト・レジスタもこれと同じ構成である。

次に、第７ｂ図をも参照して、これらのシフト・レジスタの動作について説明する。まずサイクル４０において、ＵＯＢ７００及びＬＯＢ７５０の各シフト・レジスタのすべてのラッチに接続されているＬＤＯＢ線及び$\overline{\text{ＬＤＯＢ}}$線へ信号が印加され、これによりＵＤＲ２００からＵＯＢ７００への３２ビット出力の並列転送及びモジュロ２加算器６５０～６６４からＬＯＢ７５０への３２ビット出力の並列転送が同時に行なわれる。

ＵＯＢ７００及びＬＯＢ７５０へロードされた６４ビットの被暗号化ブロックは、そこで一時に８ビット・バイトずつ並列－直列変換を受け、各シフト・レジスタの最終段のビット内容が、１つの８ビット・バイトとしてＰボックス８００へ印加される。Ｐボックス８００では、暗号化されたデータ・ビットをデータ・バス・アウトの適切なビット線へ接続するために、各８ビット・バイトに対する最後の順形置換が行なわれる。ＵＯＢ７００及びＬＯＢ７５０における並列－直列変換は、８個の各シフト・レジスタ０ＵＯＢ～３ＬＯＢの第２段から第８段までに、ＤＯＢ線及び$\overline{\text{ＬＤＯＢ}}$線を介して信号を印加することによつて実行され、かくして、サイクル４１～４７の間に、各シフト・レジスタにあるデータ・ビットが１ビット位置ずつシフト・ダウンされる。各々の最終段からのビットで構成された８ビット・バイトは、上述のようにＰボックス８００で置換された後、データ・バス・アウトへ出力される。サイクル４８において、６４ビットの暗号化されたブロックの最後のバイトが転送され、これで暗号化プロセスが完了する。

第７ａ及び７ｂ図には、次のメッセージ・ブロックを暗号化するためのサイクルは示されていないが、暗号化されるべきメッセージ・ブロックがあと幾つあつても、上と同じような方式で暗号化することができる。従つて、データの最初のメッ

セージ・ブロックが暗号化されている間に、もし次のメッセージ・ブロックが暗号装置に受取られると、このメッセージ・ブロックはＵＩＢ１００及びＬＩＢ１５０にロードされる。サイクル５９が終つて、最初の暗号化プロセスの最後の繰返し操作が完了すると、暗号キーはＵＫＲ３５０及びＬＫＲ４００内で完全に１回転されて、元の状態に戻され、従つてデータの次のメッセージ・ブロックの暗号化を制御する準備ができている。最初の暗号化プロセスのサイクル６０において、暗号化された最初のメッセージ・ブロックがＵＯＢ７００及びＬＯＢ７５０へ転送されている間に、第７ｂ図に概略で示されるように、ＩＢＴ線及びＬＤＲ線へ信号を印加することにより、次のメッセージ・ブロックをＵＤＲ２００及びＬＤＲ２５０へ転送することができ、そして次の暗号化プロセスは、最初のメッセージ・ブロックがＵＯＢ７００及びＬＯＢ７５０からドロップス８００を介してデータ・バス・アウトへ転送されている間に、開始され得る。もし暗号装置に対するメッセージ・ブロックの伝送速度が高くなり過ぎて、前のメッセージ・ブロックが入力バッファからデータ・レジスタへ転送されてしまう前に次のメッセージ・ブロックが受信されるような状態が生じ得るならば、このような状態を知らせる（例えば、使用中信号を出す）ことのできる回路を設けなければならない。これは、後続のデータ・メッセージ・ブロックが暗号装置の動作速度において、同期的に伝送されるのを可能にする。

解読プロセス

本発明に従う暗号装置において、６４ビットの暗号化されたデータ・メッセージ・ブロックを解読するための解読プロセスは、暗号化プロセスで使用されたのと同じ暗号キーの制御のもとに、同様な１６回の繰返し操作を実行することによつて達成される。しかしながら、解読プロセスにおいては、暗号キーは、暗号化プロセスの場合のように、最初の繰返し操作前に事前シフトされるのではなく、最後の繰返し操作後に事後シフトされる。

更に、暗号キーは、前記の表５に示されるシフト計画に従つて、暗号化プロセスの時とは反対の方向にシフトされる。これは、暗号化プロセスにおいて実行されたすべての繰返しを元に戻して、元のメッセージ・ブロックと同一の６４ビットのメッセージ・ブロックを再生するように、解読繰返し操作時における暗号キー・ビットの適切な並列を確実に行なわせるものである。

第３ａ～３ｄ図及び第７ａ図を参照するに、前と同じようにサイクル０～７において、暗号化されたデータ・メッセージ・ブロックはデータ・バス・インを介して受信された後、ＵＩＢ１００及びＬＩＢ１５０へバッファされ、そして暗号キーはＵＫＲ３５０及びＬＫＲ４００へロードされる。続くサイクル８では、暗号化されたメッセージ・ブロックがＵＩＢ１００からＵＤＲ２００へ及びＬＩＢ１５０からＬＤＲ２５０へ各々並列に転送される。暗号化プロセスの時と同様に、サイクル９において、ＵＤＲ２００に記憶されている暗号化されたメッセージ・ブロックの第１半分が、選択された１組の暗号キー・ビットと共に被ブロック暗号処理操作で使用され、その結果はモジュロ２加算器６５０～６６４へ送られて、ＬＤＲ２５０に記憶されているメッセージ・ブロックの第２半分を変更するのに使用される。次のサイクル１０では、ＬＢ線へ印加される第１信号及びＬＤＲ線へ印加される信号により、暗号化されたメッセージ・ブロックの変更された第２半分が、このメッセージ・ブロックの第１半分に代つてＵＤＲ２００へ記憶され、これと同時に、ＵＤＲ２００に記憶されていた第１半分は、暗号化されたメッセージ・ブロックの第２半分に代つてＬＤＲ２５０へ移される。これで、解読プロセスの次の繰返し操作に対する準備ができたことになる。

解読プロセスの２回目の繰返し操作は、サイクル１０、１１及び１２で実行され、サイクル１０の間に暗号キー・ビットを１ビット位置だけシフト・ダウンすることによつて開始される。暗号キー・ビットのシフト・ダウンは、ＳＲＲ線を介してＵＫＲ３５０及びＬＫＲの第１段へ印加される

第１信号、ＳＲ線を介して段りの段へ印加される第１信号、並びにＬＤＫ線を介してすべての段へ印加される信号の制御のもとに行なわれる。ＳＲ線上の第１信号は、ＬＤＫ線上の信号と協働して、ＵＫＲ３５０及びＬＫＲ４００の各々の最終段のビット内容を各々の第１段へ転送させ、一方ＳＲ線上の第１信号は、ＬＤＫ線上の信号と協働して、ＵＫＲ３５０及びＬＫＲ４００の各段のビット内容を後続の段へ転送させる。これにより、暗号キー全体の１ビット位置のシフト・ダウンが完了され、解読プロセスの２回目の繰返し操作のための新しい暗号キー・ビットの組が得られる。この２回目の繰返し操作は、暗号化プロセスのところで説明したのと同じようにして、サイクル１２で完了される。

図面の第５に示されるように、解読プロセスの３回目の繰返し操作の開始時には、暗号キーは２ビット位置だけシフトされていなければならない。従つて、サイクル１１の間に、ＳＲＲ線及びＳＲ線へ第２信号を印加し且つＬＤＫ線へ信号を印加することによつて、暗号キーの１回目のシフト動作が行なわれ、これにより暗号キーは１ビット位置だけシフト・ダウンされる。暗号キーの２回目のシフトは、サイクル１２において、ＳＲＲ線及びＳＲ線へ第３信号を印加し且つＬＤＲ線へ信号を印加することにより行なわれる。同様にして、また所定のシフト計画に従つて、解読プロセスの後段の繰返し操作が実行され、サイクル４０で最初のプロセスが完了する。ただし、暗号化プロセスのところでも説明したように、１６回目の繰返しにおいては、ＬＢ線へ信号が印加されないので、メッセージ・ブロックの第１半分及び第２半分の出現は行なわれない。次のメッセージ・ブロックの解読に対する準備のため、サイクル４０の間に、暗号キーの最後シフトが実行され、これにより暗号キーはＵＫＲ３５０及びＬＫＲ４００内で完全に１回転されて、元の形に戻される。次いで、サイクル４１～４８の間に、解読されたデータ・メッセージ・ブロックは、ＵＤＲ２００及びモジュロ２加算器６５０～６６４の出力からＵＯＢ７０Ｄ及びＬＯＢ７５０へ各々並列に転送された後、Ｐボックス８００を介して一時に８ビット・バイトずつデータ・バス・アウトの方へ転送される。６４ビットの解読されたデータ・メッセージ・ブロックの最後のバイトは、サイクル４８で出力され、かくして解読プロセスが完了する。暗号化プロセスの時と同様、第７ａ及び７ｂ図には示されていないが、後続の暗号化されたデータ・メッセージ・ブロックも同じようにして解読することができる。暗号化プロセスの間にモジュロ２加算器６５０～６６４で実行されたモジュロ２加算は、解読プロセスでのモジュロ２加算によつて逆転されるような自己逆転プロセス（self-reversing process）であることに注意されたい。

以上説明した本発明の実施例においては、一連のモジュロ２加算器５００～５１４が使用されていたが、該ブロック暗号処理操作は、このようなモジュロ２加算器の使用だけに限定されるものではなく、４８ビットの出力を与えるものであれば、任意の他の加算器又はこれらの加算器の組合わせを使用することができる。更に、本発明に従う暗号装置の構成は、データ・メッセージ・ブロック及び暗号キーのビット数に応じて、容易に変更され得るものであり、上述の６４ビットの例に限定されるものではない。また本発明に従う暗号装置は、暗号化及び解読の一方のみを実行するだけでなく、単に動作を逆にするだけで、両方のプロセスを同じ装置で実行し得るものである。

4.図面の簡単な説明

第１図はデータ処理環境における暗号装置の設置場所を例示したブロック図。第２図は本発明に従う暗号装置の実施例を示したブロック図。第３図は第３ａ乃至３ｊ図のつながりを明らかにしたブロック図。第３ａ乃至３ｊ図は本発明に従う暗号装置の詳細なブロック図。第４図は本発明で使用されるラッチ回路の具体例を示した回路図。第５図は第４図のラッチ回路の動作の様子を示したタイミング図。第６図は本発明で使用されるＰボックスの詳細を示した回路図。第７図は第７ａ及び７ｂ図のつながりを明らかにしたブロック図。

第7a及び7b図は暗号化及び解読プロセスのタイタルを示したタイミング図、第8図は暗号化及び解読プロセスの繰返しの様子を示したブロック図である。

50…Pボックス、60…タイミング、100…上部入力バッファ（UIB）、150…下部入力バッファ（LIB）、200…上部データ・レジスタ（UDR）、250…下部データ・レジスタ（LDR）、300…Pボックス、350…上部キー・レジスタ（UKR）、400…下部キー・レジスタ（LKR）、450…Pボックス、500～514…モジュロ2加算器、550～564…Sボックス、600…Pボックス、650～664…モジュロ2加算器、700…上部出力バッファ（UOB）、750…下部出力バッファ（LOB）、800…Pボックス。

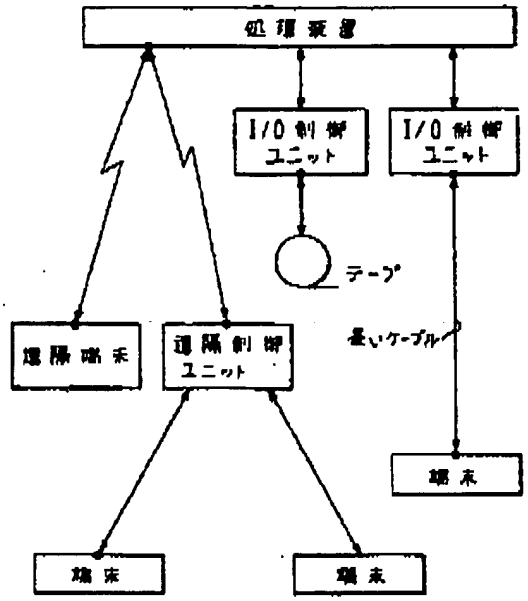


FIG. 1

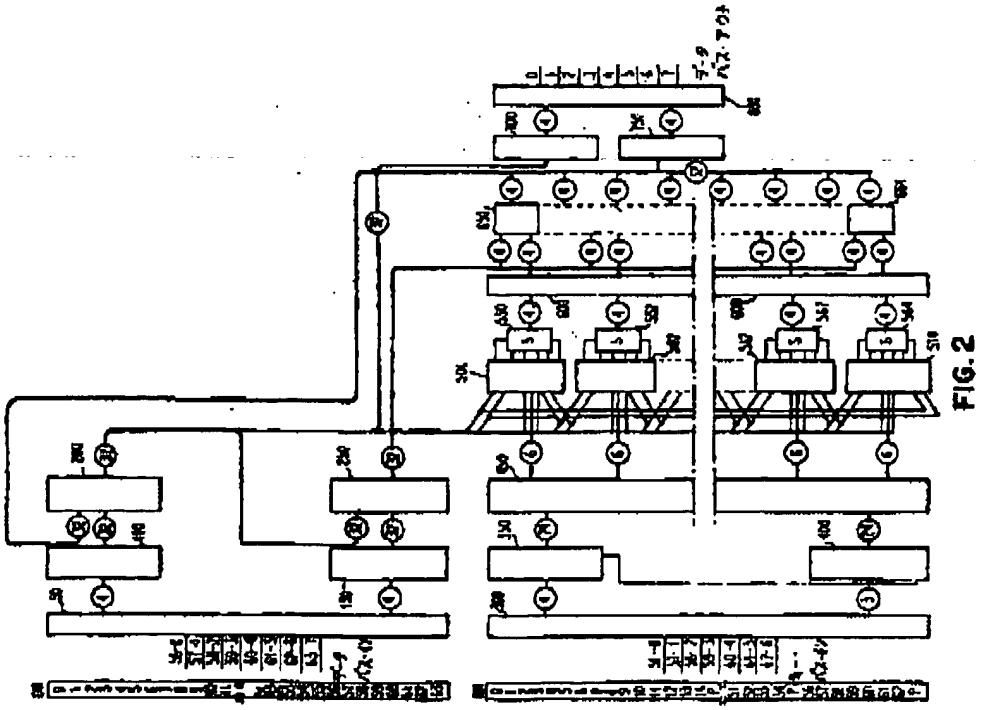


FIG. 2

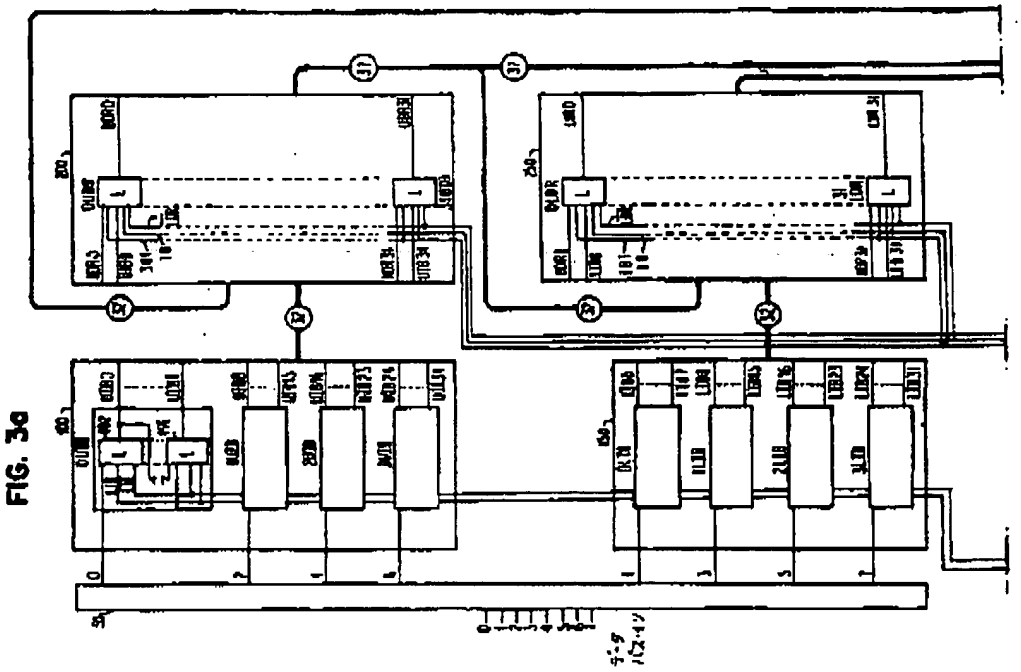


FIG. 3a

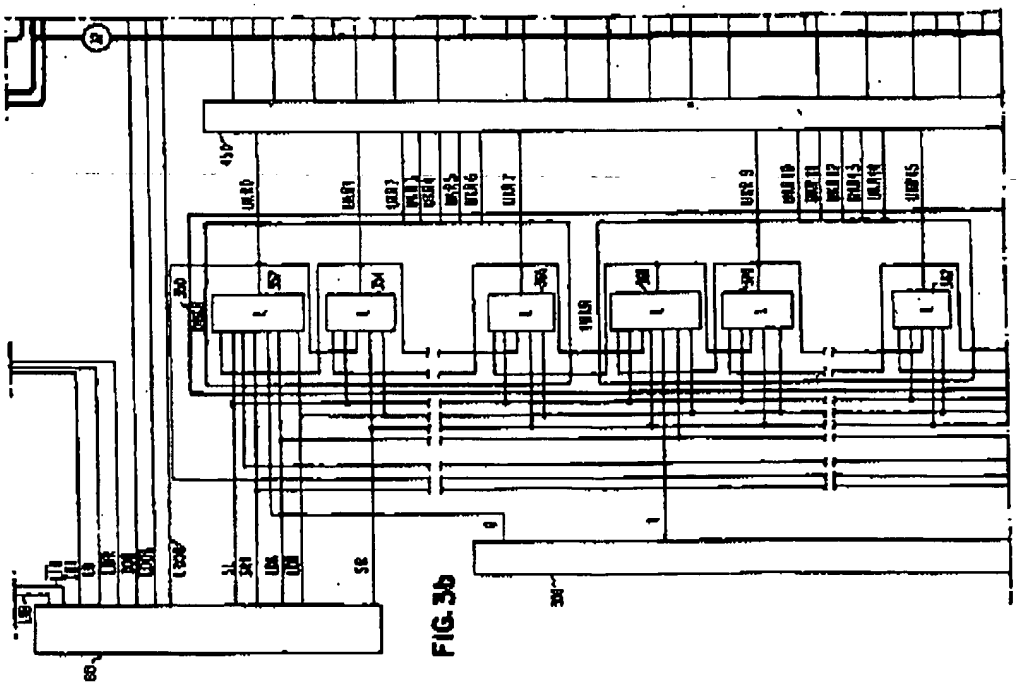


FIG. 3b

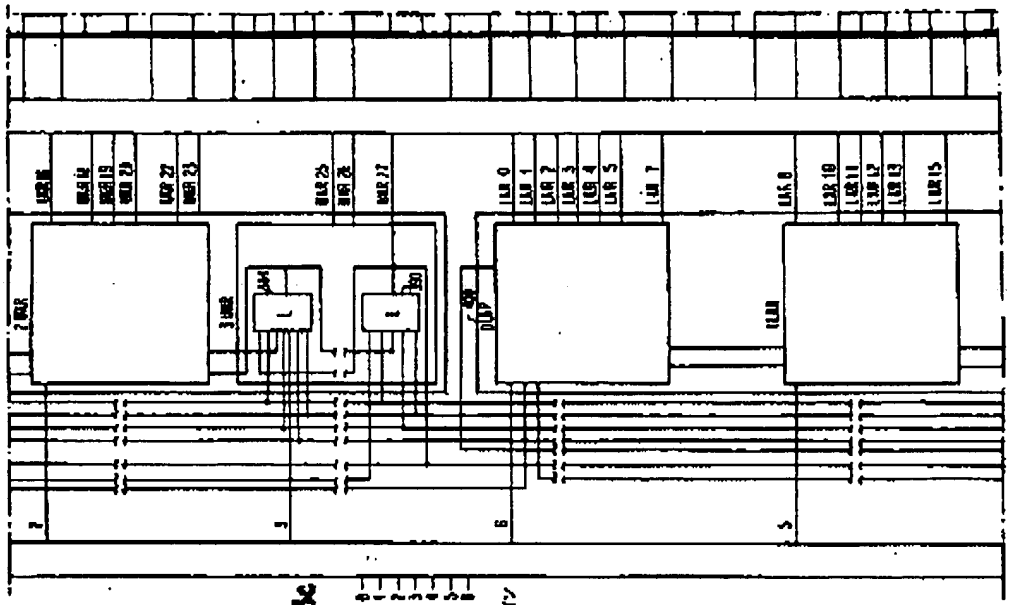


FIG.3c

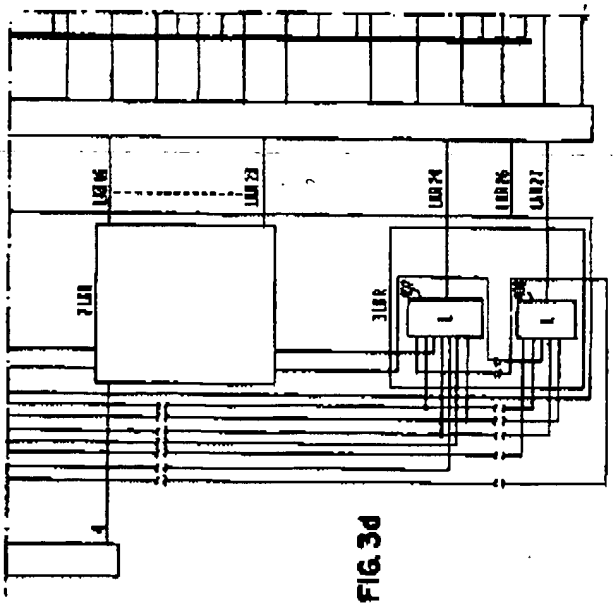


FIG.3d

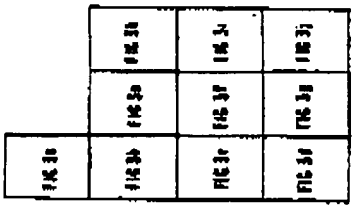


FIG.3

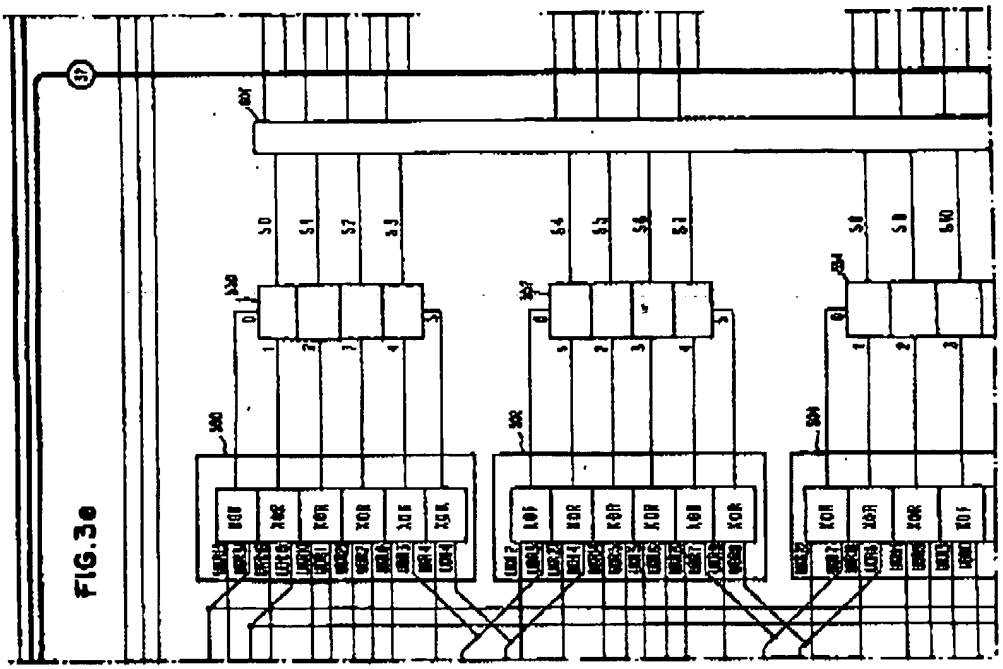


FIG.30

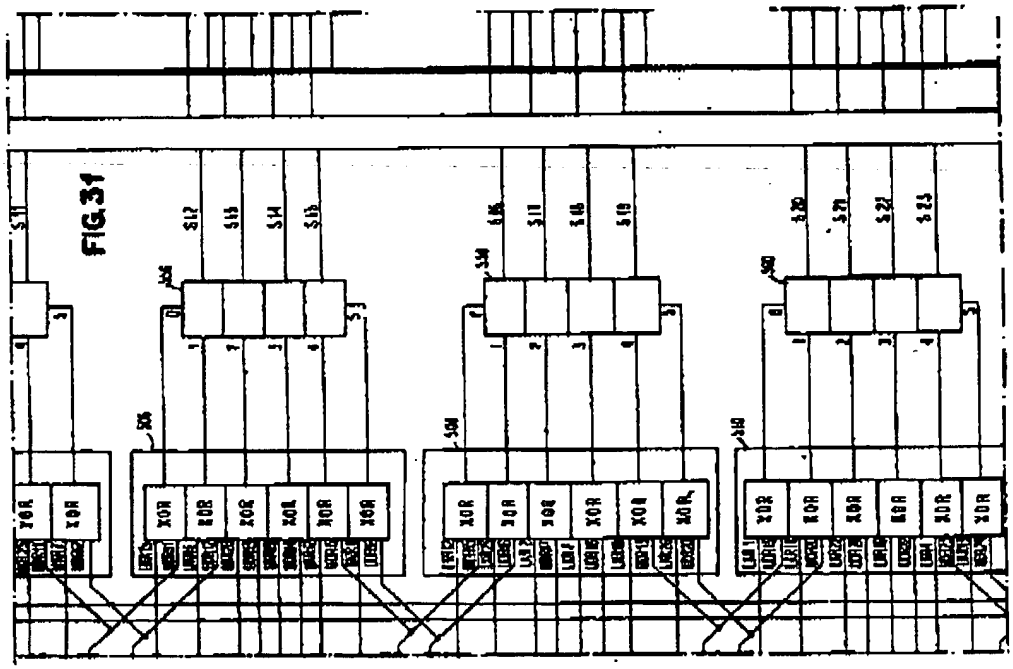


FIG.31

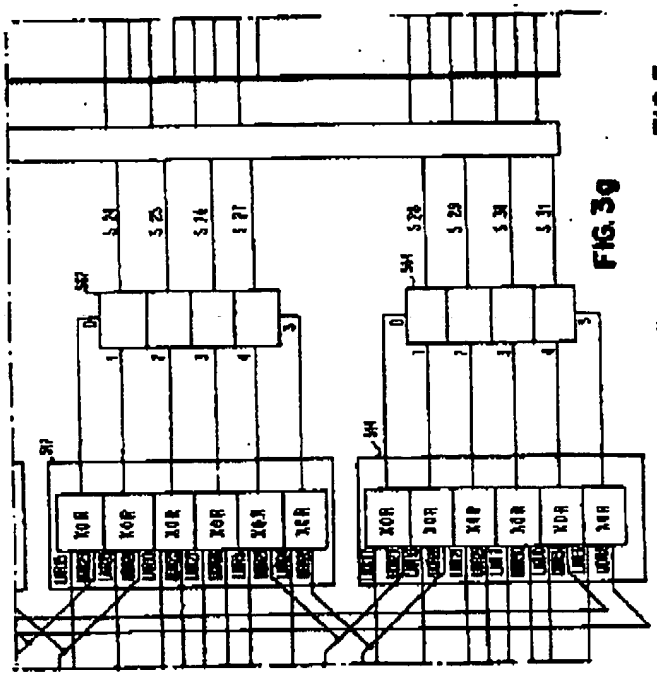
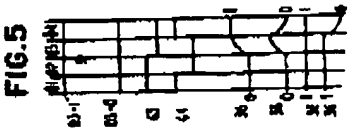


FIG.3g



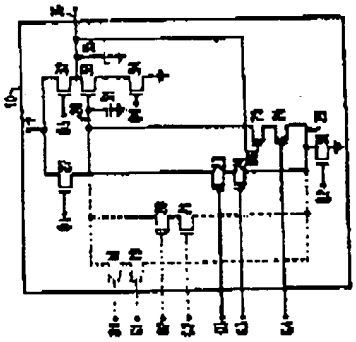


FIG.4

FIG.5

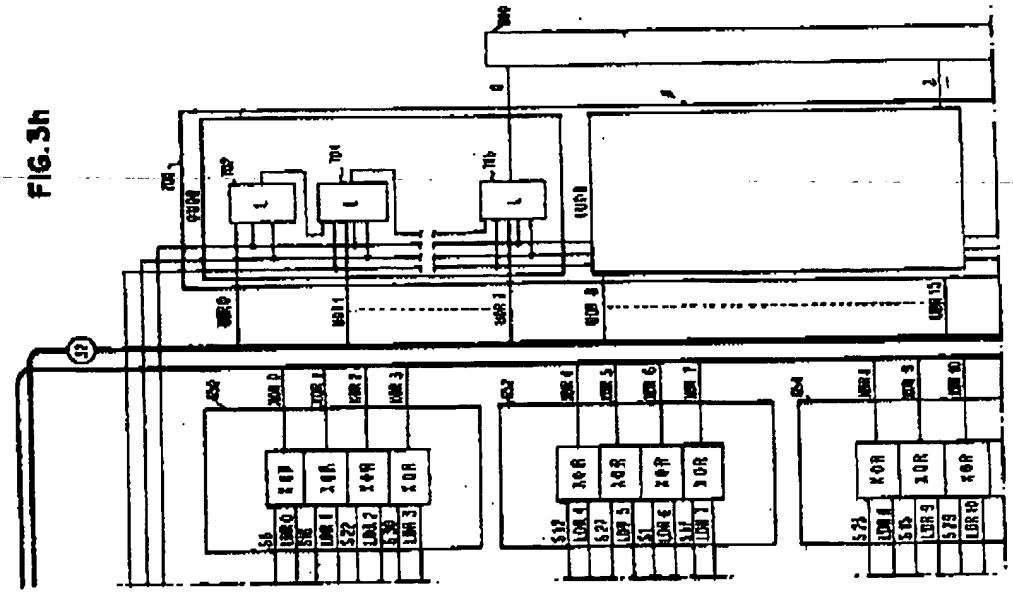
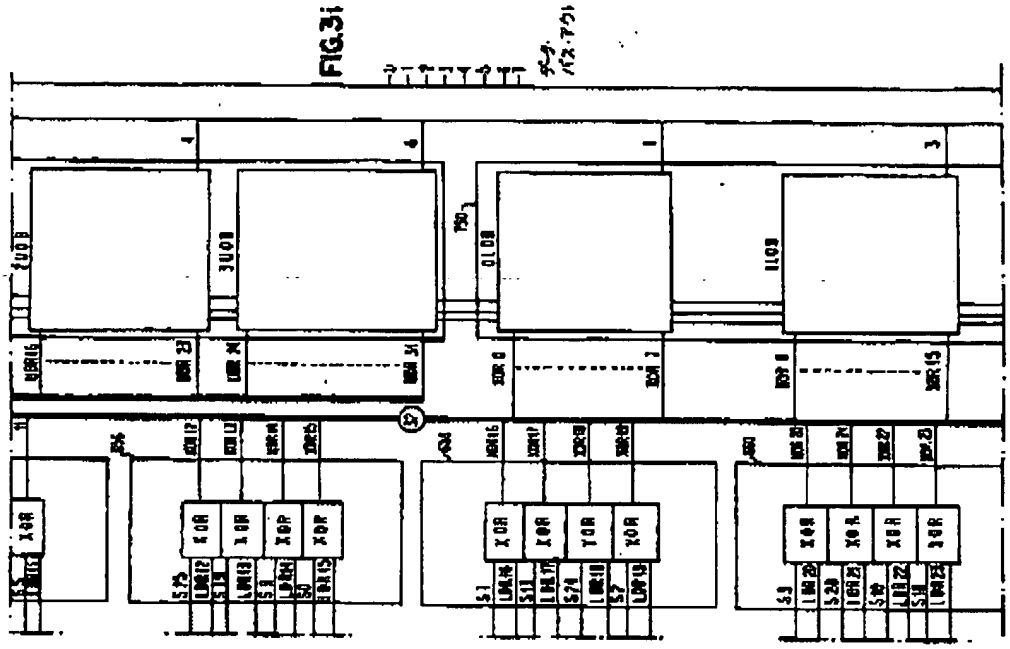


FIG.3h

FIG.3i



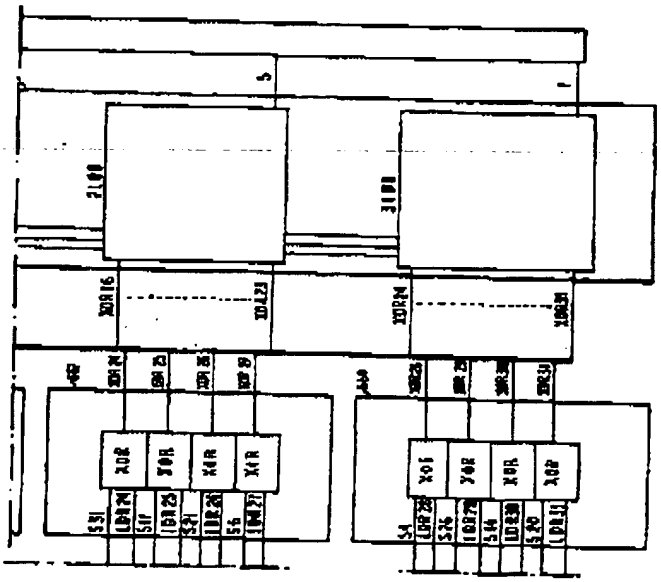


FIG.3j

FIG.7

FIG.7a	FIG.7b

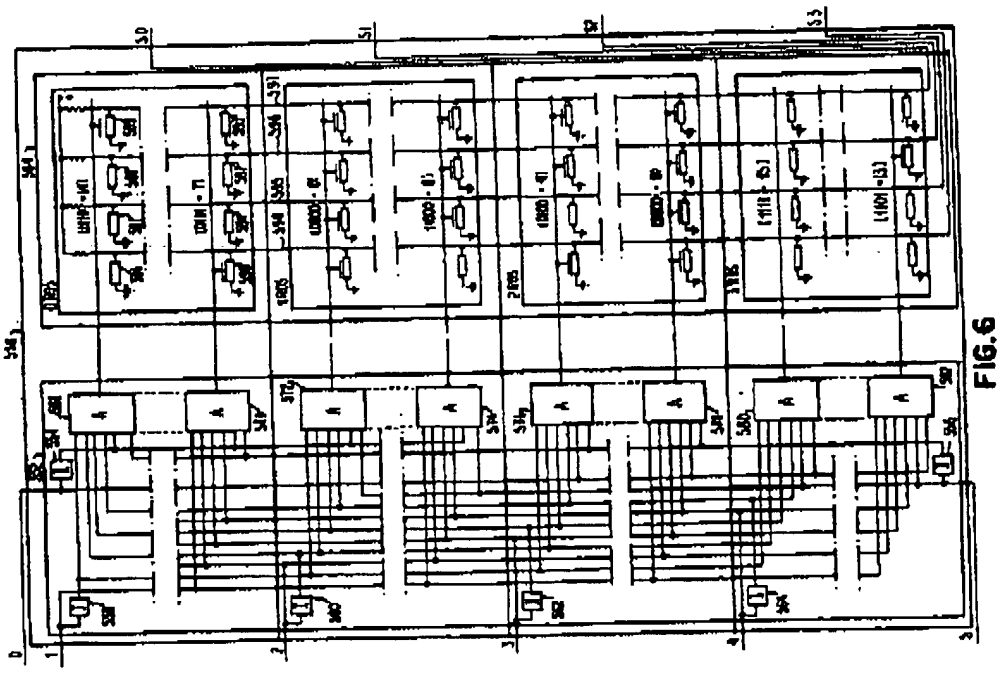


FIG.6

FIG. 7a

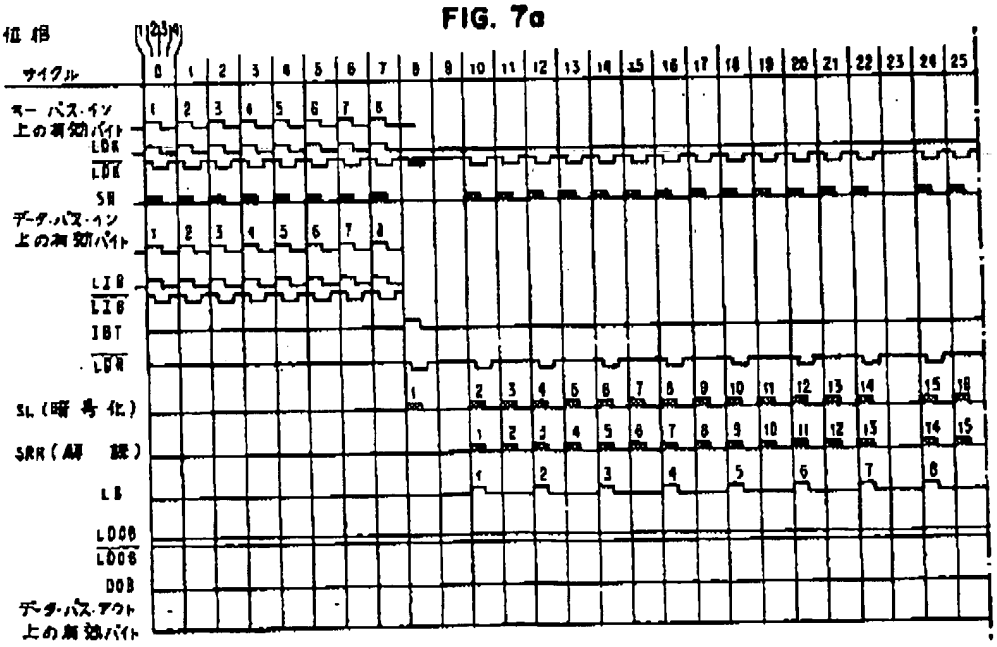

位相
サイクル
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
キー・バス・イン上の有効バイト
LDR
LDR
SR
データ・バス・イン上の有効バイト
LIB
LIB
IBT
LBR
SL（暗号化）
SRR（解読）
LB
LDOB
LDOB
DOB
データ・バス・アウト上の有効バイト

FIG. 7b

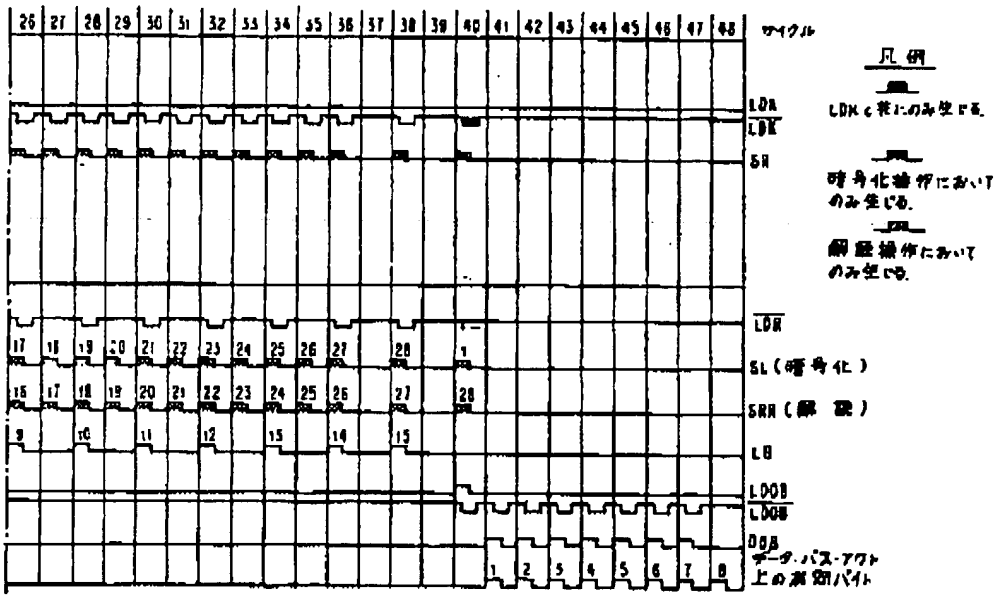
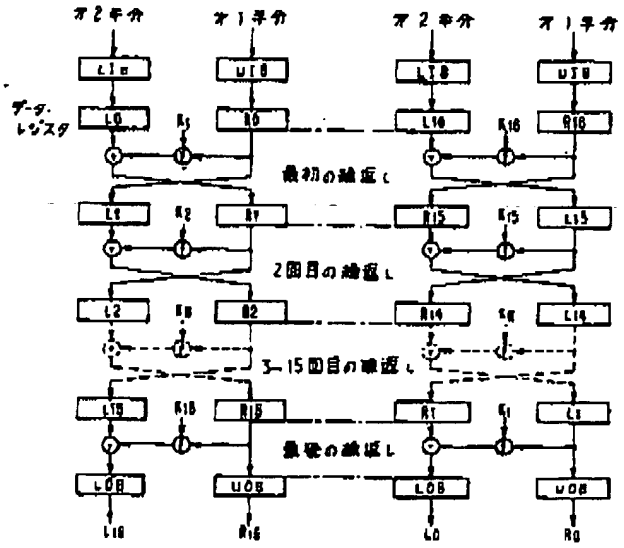


FIG. 8



◇前記以外の発明者又は代理人

(1) 発明者

住 所 アメリカ合衆国ニューヨーク州キングストン、ボックス223－11、アール ディー2、ルート28番地

氏 名 カール・エイケ・ダブリュー・メイヤー

住 所 アメリカ合衆国ニューヨーク州ウエスト・ハーレー、フィールドストーン・ロード12番地

氏 名 ロバート・エル・パワーズ

住 所 アメリカ合衆国ニューヨーク州ウッドストック、ホリー・ヒル・ドライブ7番地

氏 名 ジョン・エル・スミス

住 所 アメリカ合衆国ニューヨーク州ウッドストック、ホワイトハイ・ドライブ27番地

氏 名 ワオルター・エル・タフチマン

Jpn Pat. Appln. KOKAI Publication No. 51-108701

Filing No.: 51-16096
Filing Date: February 18, 1976
Applicant: International Business Machines Corporation
KOKAI Date: September 27, 1976
Request for Examination: Filed
Int.Cl.: H 04 K 1/00
H 04 L 9/00
G 06 F 3/00

Lines 7-16 of Upper Left Column of Page 3

The present invention provides an encrypting apparatus that can perform encrypting processing (encrypting or decrypting) with respect to a 32-bit data block under the control using one arbitrarily-selected encrypting key. The encrypting apparatus encrypts data by expanding a 32-bit data block into a 48-bit data block. The original data block includes eight segments each having four data bits, and the expanded data block includes eight segments each having six data bits.

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.